Web Application Container Server White Paper

2009-03-12

Introduction to Web Application Container Server (WACS)

Web Application Container Servers (WACS) provide a platform for hosting SAP BusinessObjects Edge Series 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 earlier required for configuring application servers and deploying web applications. It also provides a simplified, consistent administrative interface.

Web applications, such as the CMC, are automatically deployed to WACS. You cannot deploy Business Objects or external web applications to WACS, either manually or by using the wdeploy tool.

Related Topics

- *Common tasks* on page 5

What is supported on WACS?

The following services are fully supported on WACS:

- CMC service (includes viewing Crystal Reports, Web Intelligence documents, and Desktop Intelligence documents)
- Web Services SDK and QaaWS
- Business Process BI Web Services
- Live Office
- InfoView
- Voyager

When do I need WACS?

If you want to use .NET InfoView, and if 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).

You need not install WACS if you are using a supported Java application server to deploy SAP BusinessObjects Edge Series web applications.

Note:
WACS is supported only on Windows operating systems.

What are the advantages of using WACS?

The following are the advantages of using WACS to host CMC:

- WACS requires minimum effort to install, maintain, and configure.
- All hosted applications are predeployed on WACS. As a result, you need not deploy applications manually.
- If you are using WACS, then you need not administer and perform maintenance tasks for the Java application server.
- WACS provides an administrative interface that is consistent with other SAP BusinessObjects servers.

Common tasks

Task	Description	Related topics
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 and removing additional WACS* on page 9
How can I create an environment where I can easily recover from a CMC that is not configured properly?	Create a second WACS instance and use this instance to define a configuration template. If the primary WACS is not configured properly, then you can use either the second WACS until you configure the first server, or apply the configuration template to the first server.	*Adding and removing additional WACS* on page 9
How can I improve the security of communication between clients and WACS?	Configure HTTPS on WACS.	• *Configuring HTTPS/SSL* on page 15 • *Using WACS with firewalls* on page 53
How can I improve the security of communication between WACS and other SAP Business Objects Edge Series servers in my deployment?	Configure SSL communication between WACS and other SAP BusinessObjects Edge Series servers in your deployment.	

Task	Description	Related topics
Can I use WACS with HTTPS and a reverse proxy?	You can use WACS with HTTPS and a reverse proxy by creating two WACS instances and configuring both the servers with HTTPS. Use the first WACS instance for communication in your internal network, and the second WACS instance for communication with an external network through a reverse proxy.	*Configuring WACS to support HTTPS with a reverse proxy* on page 53
How does WACS fit in my IT environment?	WACS can be deployed in an IT environment that includes web servers, hardware load balancers, reverse proxies, and firewalls.	• *Using WACS with other web servers* on page 51 • *Using WACS with a load balancer* on page 52 • *Using WACS with a reverse proxy* on page 52 • *Using WACS with firewalls* on page 53
Can I use WACS in a deployment that includes a load balancer?	You can use WACS in a deployment that uses a hardware load balancer. However, WACS itself cannot be used as a load balancer.	*Using WACS with a load balancer* on page 52
Can I use WACS in a deployment that includes a reverse proxy?	You can use WACS in a deployment that uses a reverse proxy. However, WACS itself cannot be used as a reverse proxy.	*Using WACS with a reverse proxy* on page 52

Task	Description	Related topics
How can I troubleshoot my WACS servers?	If you need to determine the reasons for the poor performance of your WACS, you can view the log files and the system metrics.	• *Viewing server errors* on page 64 • *Viewing system metrics* on page 65
I do not 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. Verify whether: • HTTP, HTTP through proxy, and HTTPS ports that you specified for the WACS have been taken by other applications. • WACS has enough memory allocated to it. • WACS allows enough concurrent requests. If necessary, restore the default settings for the WACS.	• *Resolving HTTP port conflicts* on page 67 • *Changing the memory settings* on page 69 • *Changing the number of concurrent requests* on page 70 • *Restoring default settings* on page 70
Where can I find a list of WACS properties?	The “WACS properties” section in this guide provides a list of WACS properties.	*WACS properties* on page 54

Administering WACS

Installing WACS

Installing WACS on separate machines in your deployment provides better

performance and load balancing, and higher server availability. If your deployment contains machines on which two or more WACS are installed, then CMC availability is not affected by hardware or software failures on a specific machine. This is because the other WACS continue to provide CMC services.

You can install a WACS by using the SAP BusinessObjects Edge Series installation program. You can install WACS in the following ways:

- Express installation, in which WACS is automatically installed.
- Advanced installation, in which you can choose to install WACS on the "Select Web Application Server" screen by selecting the **Deploy the web components in the Web Application Container Server** option.

If you install WACS, the installation program automatically creates a server called *<NODE>*.WebApplicationContainerServer, where *<NODE>* is the name that identifies the node of your deployment. 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 in use. The default port number is 6405. If you plan to allow users outside the firewall to connect to the WACS, you must ensure that the server's HTTP port is open on the firewall.

For information about installing WACS when you are upgrading from Business Objects Crystal Decisions, see the *SAP BusinessObjects Edge Series 3.1 Installation Guide for Windows*.

Note:

The web applications hosted by WACS are automatically deployed in the following scenarios:

- when you install WACS.
- when you apply updates or hot-fixes to WACS
- when you apply updates or hot-fixes to WACS-hosted web applications

It takes several minutes for the web applications to deploy. Until the web application deployment is complete, WACS continues to be in the “Initializing” state. As a result, you cannot access web applications hosted on WACS until the web applications are fully deployed. However, you can view the state of WACS through the Central Configuration Manager (CCM).

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

Adding and removing additional WACS

The following are the advantages of adding additional WACS to your deployment:

- Faster recovery from a server that is not configured properly
- Improved server availability
- Better load balancing
- Improved overall performance

The following are ways to add additional WACS to your deployment:

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

Note:
You can deploy more than one WACS instance on the same machine. However, it is recommended that you do not run more than one WACS on a single machine at the same time, because this results in high resource utilization.

Adding a new WACS

To add a new WACS to your deployment, perform the following steps:

1. Navigate 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. In the "Create New Server" screen, click **Next**.

6. In the "Create Server" screen, perform the following steps, and then click **Create**:
   a. Select the node to which you want to add the server.

      Note:
      Only those nodes on which WACS is installed are displayed in the **Node** list.

   b. Type a server name
   c. Type a server port
   d. Type a description for the server
7. In 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 instance of WACS is created. The default settings and properties are applied to WACS.

Cloning a WACS

Cloning is an alternative way to add a new WACS instance to the same machine or to another machine in your deployment. Adding a new WACS instance creates a server with default settings, whereas when you clone a WACS, the settings in the source WACS are applied to the new WACS instance. You can clone a WACS only if you have already installed WACS on the system.

To clone a WACS, perform the following steps:

1. Navigate 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 on which WACS is installed are displayed in the **Clone to Node** list.
3. In 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 instance 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 clone 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 of the newly cloned WACS instance.

Related Topics

- *Resolving HTTP port conflicts* on page 67

Deleting WACS

You can delete a WACS instance only if the server is not currently serving the CMC. If you want to delete a WACS instance from your deployment, you must log into a CMC from another instance of WACS or a Java application server, and perform the following steps:

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

Adding and removing services to WACS

Adding a CMC service to WACS

After you install WACS, a Central Management Console (CMC) service is automatically added to your deployment. You need not 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.

Adding a CMC service to a WACS requires you to stop 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 adding a service to the other WACS.

To add a CMC service to WACS, perform the following steps:

1. Navigate 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 WACS 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 attempt to stop the WACS that is currently serving a CMC, a warning message appears. Do not proceed unless you have at least one additional CMC service running on another WACS in your deployment. If another WACS instance is running the CMC service, click **OK** to stop the WACS.
5. Right-click the WACS you stopped, and click **Select Services.**

   The "Select Services" screen appears.
6. From the "Available services" list, select **Central Management Console Service**, and click **>** to add it to WACS.
7. Click **OK**.
8. To start WACS, right-click and select **Start Server**.

The CMC service is added to the WACS. The default settings and properties for the CMC are applied.

Removing a CMC service from WACS

When you remove a CMC service from WACS, you must ensure that it is not the only CMC service running on WACS in your deployment. You cannot delete the last CMC service from WACS. When you remove a CMC service from WACS, you must ensure that the WACS also hosts other services. If you want to remove the last service from a WACS, delete the WACS itself.

To remove a CMC from WACS, perform the following steps:

1. Navigate 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 WACS to ensure that a CMC service is present.
3. Click **Cancel** to return to the "Servers" screen.

4. To stop WACS from which want to remove the CMC, right-click the server, and click **Stop Server**.

   If you attempt to stop the WACS that is currently serving a CMC, a warning message appears. Do not proceed unless you have at least one additional CMC service running on another WACS in your deployment. If another WACS instance is running the CMC service, click **OK** to stop the WACS.
5. Right-click the stopped WACS, and click **Select Services**.
6. On the "Services" list, select **Central Management Console Service**, and click **<** to remove it from WACS.
7. Click **OK**.
8. To start WACS, right-click and select **Start Server**.

The CMC service is removed from the WACS.

Adding a web service to a WACS

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 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.

To add a web service to a WACS, perform the following steps:

1. Navigate 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 click **Stop Server**.

   If you are attempting to stop the WACS that is currently serving the CMC to you, a warning message appears. Do not 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 click **Start Server**.

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

Removing a web service from a WACS

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.

To remove a web service from a WACS, perform the following steps:

1. Navigate 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. Do not 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 click **Start Server**.

The web service is removed from the WACS.

Configuring WACS

Configuring HTTPS/SSL

You can use the Secure Sockets Layer (SSL) protocol and HTTPS for network communication between clients and WACS in your SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series servers in your deployment. This is known as CORBA SSL. 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 in 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 if you want to use SSL to secure the network communication in your deployment, you must create two instances of WACS. For more information, see *Using WACS with a reverse proxy*.

To configure HTTPS/SSL on WACS, you must perform the following tasks:

- Generate or obtain a PKCS12 certificate store or JKS keystore that 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.
- If you have a certificate store and 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 52

Generating a PKCS12 certificate file store

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

To generate a PKCS12 certificate file store, perform the following steps:

1. Log into the system that hosts WACS by using administrator credentials.
2. In IIS, request a certificate from Certificate Authority. For information on requesting a certificate, see the IIS help documentation.
3. Select **Start** > **Run**.
4. Start the MMC by typing mmc, and click **OK**.
5. Add Certificates Snap-in to the MMC:
   a. In the **File** menu, click **Add/Remove Snap-in**.
   b. Click **Add**.
   c. In 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.
6. In the MMC, expand **Certificates**, and select the certificate that you want to use.
7. In the **Action** menu, select **All Tasks** > **Export**.

   The "Certificate Export Wizard" starts.
8. Click **Next**.
9. Select **Yes, export the private key**, and click **Next**.
10. Select **Personal Information Exchange - PKCS #12 (.PFX)**, and click **Next**.
11. 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.

Generating a Certificate Trust List

To generate a Certificate Trust List, perform the following steps:

1. Log into the system that hosts WACS by using administrator credentials.
2. To start the Microsoft Management Console (MMC), perform the following steps:
   a. Select **Start** > **Run**.
   b. Type mmc, and click **OK**.
      The "Console" screen appears.
3. In the "Console" screen, perform the following steps to add Internet Information Services Snap-in:
   a. From **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, locate the website for which you want to create the Certificate Trust List.
5. Right-click the website, 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. Type 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.

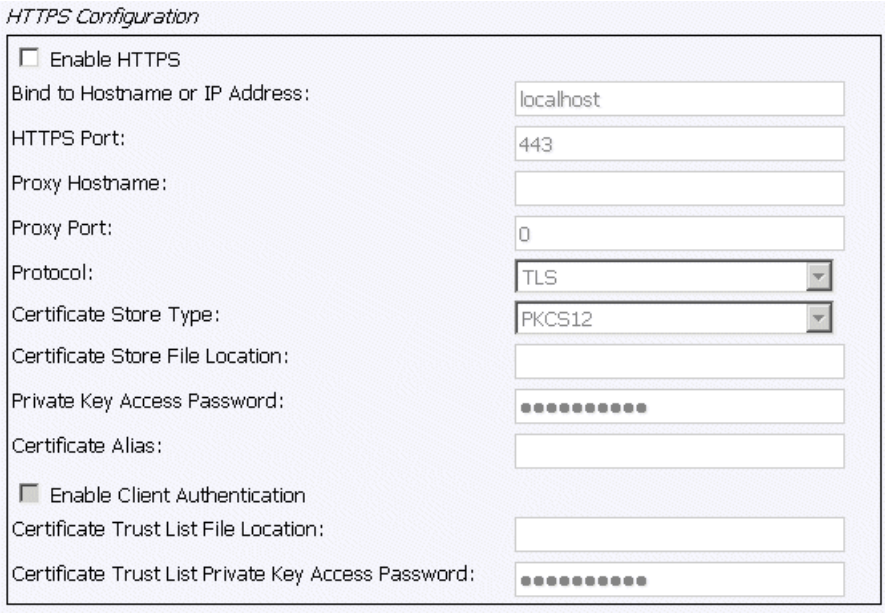
Configuring HTTPS/SSL

Before you configure HTTPS/SSL on your WACS, make sure that you have already created a PCKS12 file or JKS keystore. You must also ensure that you have copied or moved the file to the system that hosts WACS.

To configure HTTPS/SSL, perform the following steps:

1. Navigate to the"Servers" management area of CMC.
2. Double-click the WACS for which you want to enable HTTPS.

   The "Properties" screen appears.
3. In the "HTTPS Configuration" section, select the **Enable HTTPS** checkbox.



4. In the **Bind to Hostname or IP Address** field, specify the IP address to which WACS must bind.

   HTTPS services are provided through the IP address that you specify.

5. In the **HTTPS Port** field, specify a port number for WACS to provide HTTPS service. Ensure that the port you specify is not being used by other servers or applications. If you want users to connect to WACS from outside a firewall, ensure that the specified 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. In the **Protocol** list, select a protocol. The supported options are:
   - **SSL**

     SSL (Secure Sockets Layer) protocol, used to encrypt network traffic.
   - **TLS**

     TLS (Transport Layer Security) protocol, is a new and enhanced protocol.

     The only difference between SSL and TLS is that TLS has a stronger encryption algorithm.

8. In the **Certificate Store Type** field, specify the file type for the certificate. The supported options are:
   - **PKCS12**

     Select this option if you want to work with Microsoft tools.
   - **JKS**

     Select this option if you want to work with Java tools.
9. In the **Certificate Store File Location** field, specify the path where you have copied or moved the certificate file store or Java keystore file.
10. In the **Private Key Access Password** field, specify the password.

    PKCS12 certificate store and JKS keystore have private keys that are password protected, to prevent unauthorized access. You must specify the password to access the private keys, so that WACS can access the private keys.

    Note:
    SAP BusinessObjects recommends that you use a certificate file store or keystore that contains a single certificate or the certificate that you want to use in a list. However, if you are using a certificate file store or keystore that contains more than one certificate, and if this certificate is not the first one in the file store, then, in the **Certificate Alias** field, specify the alias for the certificate.
11. If you want WACS to accept only HTTPS requests from certain clients, enable client authentication.

    Client authentication does not authenticate users. However, it ensures that WACS serves HTTPS requests only to certain clients.

    To enable client authentication, perform the following steps:

    a. Select **Enable Client Authentication**.
    b. In the **Certificate Trust List File Location** field, specify the location of the PCKS12 file or JKS keystore that contains the Certificate 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 regulates access to the private keys in the Certificate Trust List file.

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

12. Click **Save & Close**.
13. Navigate to the "Metrics" screen, and ensure that the 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
- AD Kerberos Single Sign-On

Configuring AD Kerberos for WACS

Before you configure AD Kerberos authentication for WACS, you must first configure your system to support AD. Configuring your system to support AD involves the following tasks:

- 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 have configured the system that hosts 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 system that hosts WACS.

Related Topics

- *Using AD users group* on page 23
- *Windows AD security plug-in* on page 22
- *Mapping AD accounts* on page 23
- *Setting up a service account* on page 30
- *Setting up constrained delegation* on page 33
- *Configuring the servers* on page 34
- *Enabling Kerberos authentication in Windows AD plug-in for WACS* on page 37
- *Creating configuration files* on page 39
- *Configuring WACS for AD Kerberos* on page 42
- *Configuring WACS for AD Kerberos single sign-on for Web Services SDK and QaaWS* on page 50

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 SAP BusinessObjects Edge Series. It also enables SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series supports domains within multiple forests.

Using AD users group

SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series. This enables the administrator to map previously created user accounts and groups, instead of setting up each user and group within SAP BusinessObjects Edge Series.

Note:
AD authentication works only 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, SAP BusinessObjects Edge Series supports AD authentication for user and group accounts. However, before users can use their AD user name and password to log on to SAP BusinessObjects Edge Series, their AD user account needs to be mapped to SAP BusinessObjects Edge Series. When you map an AD account, you can choose to create a new SAP BusinessObjects Edge Series account or link to an existing SAP BusinessObjects Edge Series account.

Mapping AD users and groups and configure the Windows AD security plug-in

Regardless of which protocol is used, perform the following steps to authenticate AD users:

1. Navigate 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 will be populated with the AD Administration names.

5. Enter the name and password of an enabled domain user account. SAP BusinessObjects Edge Series 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)

   SAP BusinessObjects Edge Series 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 expired or the account is disabled).

6. Enter the default AD domain details in the **Default AD Domain** field.
   - 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 SAP BusinessObjects Edge Series through 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 SAP BusinessObjects Edge Series. Therefore, they will not be able to access SAP BusinessObjects Edge Series.

8. Click **Add**.

   The group is added to the list.

   You can skip the configuration of the "Authentication Options", "Synchronization of Credentials" and "SiteMinder Options". For information

on how to configure Windows AD with Kerberos, NTLM, or SiteMinder refer to, *BusinessObjects Enterprise Administrator's Guide*

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

        Use this option when you know users have an existing SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series account, or who do not have the same name in their SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series accounts. Select one of the following options:
      - **Create new aliases when the Alias Update occurs**

        Use this option to automatically create a new alias for every AD user mapped to SAP BusinessObjects Edge Series. New AD accounts are added for users without SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series. SAP BusinessObjects Edge Series does not automatically create aliases and SAP BusinessObjects Edge Series accounts for all users. Instead, it creates aliases (and accounts, if required) only for users who log on to SAP BusinessObjects Edge Series.

c. In "New User Options", specify how new users are created by selecting one of the following options:

- **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 users 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 SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series, 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 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 SAP BusinessObjects Edge Series.

- **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 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 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 select this option, neither the group graph nor the user aliases will 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".

14. Click **Update**.

Scheduling AD updates

SAP BusinessObjects Edge Series 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 run every hour. You can specify the time, and the start and end date for the update to run.
Daily	The update will run every day or the number of days specified. You can specify the time, and the start and end date for the update to run.
Weekly	The update will run every week. It can be run once a week or several times a week. You can specify a day, time, and start and end date for the update to run.
Monthly	The update will run every month or every several months as specified. You can specify the time, and the start and end date for the update to run.
Nth Day of Month	The update will run on a specific day in the month. You can specify on which day of the month, the update should run, and also the time, and start and end date.

Recurrence pattern	Description
1st Monday of Month	The update will run on the first Monday of each month. You can specify the time, and the start and end date for the update to run.
Last Day of Month	The update will run on the last day of each month. You can specify the time, and the start and end date for the update to run.
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 the time, and the start and end date for the update to run.
Calendar	The update will run on the specified dates in a calendar that was previously been created.

Scheduling group graph updates

SAP BusinessObjects Edge Series relies on Active Directory for AD user, and group information. To minimize the volume of queries sent to AD, the AD plugin caches information about groups, and how they relate to each other, and their user membership. The group graph is recreated by default every 15 minutes if 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

SAP BusinessObjects Edge Series users can log on to the system with their AD information. To facilitate this scenario, each user object has an associated AD alias to map them to a distinct user in AD. As changes occur to the user accounts in AD, these changes has to be reflected in SAP BusinessObjects Edge Series . If a user is deleted or disabled in AD, the AD alias in SAP BusinessObjects Edge Series is deleted or disabled when the AD alias update occurs. Also, if you setup the AD plugin to **Create new aliases when the**

Alias Update occur, new AD aliases will be created when the AD alias update occurs.

If you do not schedule a update for AD alias, the alias updates will occur only when:

- a user logs on.
- selects the **Update AD Group Graph and Aliases now** option, from the "On-demand AD Update" area of the CMC.

Note:
In the user alias no AD passwords are stored.

Setting up a service account

To configure SAP BusinessObjects Edge Series 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. Service account is used to run SAP BusinessObjects Edge Series servers.

After you have set up a service account, you have to grant appropriate rights to the account , see *Granting the service account rights* on page 35.

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

- If you are using Windows 2000 Domain, see *Setting up a service account on Windows 2000 Domain* on page 31 for more information.
- If you are using Windows 2003 or 2008 Domain, see *Setting up a service account on Windows 2003 or 2008 Domain* on page 32 for more information.
- If you are using Windows 2003 or 2008 Domain, you also have the option of setting up constrained delegation. See *Setting up constrained delegation* on page 33 for more information.

Note:

- If you are setting up SSO2DB, the service account must be a domain account that has been trusted for delegation.
- In a forest with multiple domains, you can create a service account in any domain. The domain in which a service account is created can be authenticated by all other domains.All domains that trust the domain you have created the service account in will be able to authenticate.

Setting up a service account on Windows 2000 Domain

To set up a service account on Windows 2000 domain, perform the following steps:

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

   For information on creating an account on a domain controller, see *http://msdn.microsoft.com/*.

2. Right-click the user account, and 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.

Running the SPN utility on Windows 2000

To run the SPN utility on Windows 2000, perform the following steps:

1. Download the utility to your Domain controller from the following website:
   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 the command prompt, and enter the following command:

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

   - Replace *<ServiceClass>* with any desired name. For example, BOBJCentralMS (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 have configured.

Note:

- Service account name is case-sensitive.
- The SPN must be unique in the forest in which it is registered. To check if the SPN is unique 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 Windows 2003 or 2008 Domain

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

To set up a service account on Windows 2003 or 2008 Domain, perform the following steps:

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

   For information on creating an account on a domain controller, see *http://msdn.microsoft.com/*.

2. Open the command prompt, and enter the follwing command:

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

   - Replace *<ServiceClass>* with any desired name. For example, BOBJCentralMS. (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 have configured.

   Note:

   - Service account name is case-sensitive.

- The SPN must be unique in the forest in which it is registered. To check if the SPN is unique 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. Right-click on the user account, and select **Properties**.
5. Click the **Account** tab, and in the "Account options" select the **Account is tested for delegation**, and **Use DES encryption types for this account** check box.
6. 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 enables 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 enables you to limit the amount of delegation permitted. Constrained delegation for a service account enables 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.

Setting up constrained delegation for a service account

To set up constrained delegation for a service account, perform the following steps:

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 the **Delegation** tab.
7. Select the **Trust this user for delegation to specified services only** option.
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 SAP BusinessObjects Edge Series servers includes the following tasks:

Granting the service account rights

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

Note:
If you are using SSO2DB, you require a service account that has been trusted for delegation. For information about setting up a service account, see the *Setting up a service account* on page 30.

To grant the service account rights

To grant service account rights, perform the following steps:

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 SAP BusinessObjects Edge Series 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

To support Kerberos, the service account must be part of the local Administrators group.

Note:
If you are using SSO2DB, you require a service account that has been trusted for delegation. For information about setting up a service account, see the *Setting up a service account* on page 30. You must also have administrative rights on the server.

To add an account to the Administrator's group

To add an account to the Administrator's group, perform the following steps:

1. Right-click **My Computer** and click **Manage**.
2. Navigate 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 SAP BusinessObjects 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 are using SSO2DB, you require a service account that has been trusted for delegation. For information about setting up a service account, see the *Setting up a service account* on page 30.

To configure a server

To configure a server to use a service account, perform the following steps:

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 Intelligence 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 30.

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 Windows AD plug-in for WACS

To support Kerberos, you must configure the Windows AD security plug-in to use Kerberos authentication. Configuring the Windows AD plug-in involves the following tasks:

- Ensuring that Windows AD authentication is enabled
- Setting up the AD Administrator account.

  Note:
  This account requires read only access to Active Directory.

- Enabling Kerberos authentication and single sign-on, if single sign-on is required.
- Entering the Service Principal Name (SPN) for the service account.

Prerequisites

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

- *Setting up a service account* on page 30
- *Granting the service account rights* on page 35
- *Configuring the servers to use the service account* on page 36
- *Mapping AD accounts* on page 23

Configuring the Windows AD security plug-in for Kerberos

To configure the Windows AD security plug-in for Kerberos, perform the following steps:

1. Navigate to the **Authentication** management area of the CMC.
2. Double-click **Windows AD**.

   Note:
   Ensure that the **Enable Windows Active Directory (AD)** check box is selected.

3. Under **Authentication Options**, select the **Use Kerberos authentication** option.
4. Select **Cache Security context**, if you want to configure single sign-on to a database.
5. In the **Service principal name** field, enter the account and domain of the service account, or the SPN mapping to the service account.

   For example, if the Service Account is svcacct@DNS.COM and if the SPN is BOBJCentralMS/some_name@DOMAIN.COM, then `svcacct` is the name of the service account or SPN you created earlier, and `DNS.COM` is your fully qualified domain in uppercase.

   Note:
   - If you want users from domains other than the default domain to log in, 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 SAP

BusinessObjects Edge Series servers or the SPN that maps to this account.

6. To configure single sign-on, select the **Enable Single Sign On for selected authentication mode** check box.

   Note:
   If single sign-on is enabled, you must configure WACS.

7. Click **Update**.

Related Topics

- *Configuring AD Kerberos single sign-on for Web Services SDK and QaaWS* on page 45

Creating configuration files

The following are the common steps to configure Kerberos on your application server:

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

Note:

- The default Active Directory domain must be in uppercase DNS format.
- You need not download and install MIT Kerberos for Windows. Also, you do not require a keytab for your service account.

Creating the Kerberos configuration file

To create a Kerberos configuration file, perform the following steps :

1. Create a file `krb5.ini`, if it does not exist, and save the file at: `C:\WINNT`

   Note:
   However, you can save this file in a different location, and specify the location in the **Krb5.ini File Location** field on the "Properties" page, for WACS server in the CMC.

2. Enter the following information to 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 view a sample file with multiple domain entries, see *Sample Krb5.ini files* on page 41.
- In a multiple domain configuration, the `default_realm` value can be of any domain. It is recommended that you use the domain with the greatest number of users who will authenticate by using their AD accounts.

3. Save and close the file.

Creating the JAAS login configuration file

To create the JAAS login configuration file, perform the following steps:

1. Create a file `bscLogin.conf` if it does not exist, and save the file at: `C:\WINNT`.

Note:
However you can save this file in a different location, and specify the location in the **bscLogin.conf File Location** field on the "Properties" page for WACS server in the CMC.

2. Add the following information in the 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 Krb5.ini 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 configure the system that hosts WACS for AD Kerberos authentication, you must configure the WACS through the Central Management Console (CMC).

To configure WACS for AD Kerberos, perform the following steps:

1. Navigate 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

The following tasks can help you to troubleshoot Kerberos during configuration:

- Enabling logging
- Testing your Kerberos configuration

Enabling Kerberos logging

To enable Kerberos logging, performing the following steps:

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

   Note:
   The **Web Tier Configuration** icon is enabled only when you select a WACS that is not running.

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

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

Testing your Kerberos configuration

To test your Kerberos configuration, type the following in the command prompt:

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

Where `servact` is the service account and the domain under which the CMS is running, and `password` is the password associated with the service account.

For example:

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

If you have any issues, make sure that you have entered the domain, and SPN correctly.

Mapped AD user unable to log on to SAP BusinessObjects Edge Series 3.1 on WACS

You may encounter the following issues even if users have been mapped to SAP BusinessObjects Edge Series 3.1:

- *Logon failure because of different AD UPN and SAM names* on page 44
- *Pre-authentication error* on page 44

Logon failure because of different AD UPN and SAM names

A user's Active Directory ID (for example, `DOMAIN\ABC123`) has been successfully mapped to SAP BusinessObjects Edge Series. However, the user is unable to successfully log into CMC with AD authentication and Kerberos.

This problem occurs 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 and the SAM name is DOMAIN\ABC123.
- The UPN is jsmith@company and the SAM name is DOMAIN\

There are two ways to address this problem:

- Ensure that 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 the following error message: `Account Information Not Recognized`

The WACS log file contains the following error: `"Pre-authentication information was invalid (24)"`

This occurs because, the Kerberos user database is not reflecting the changes made to UPN in AD. This means 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

If you are configuring AD Kerberos single sign-on for Web Services SDK and QaaWS, make sure that you have configured WACS and the system that is hosting WACS for AD Kerberos authentication. For information on configuring AD Kerberos for WACS, see *Configuring AD Kerberos for WACS* on page 21.

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

- *Configuring your system for AD Kerberos single sign-on to Web Services SDK and QaaWS* on page 46
- *Configuring WACS for AD Kerberos single sign-on for Web Services SDK and QaaWS* on page 50

Note:
If you want to use single sign-on to Web Services SDK and QaaWS in a reverse proxy environment, refer to 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, allowing authenticated AD users to log on to SAP BusinessObjects Edge Series without explicitly entering their credentials. The single sign-on requirements depends on the way in which users access SAP BusinessObjects Edge

Series: either through 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 SAP BusinessObjects Edge Series 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 SAP BusinessObjects Edge Series 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 system 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 system that hosts WACS. Configuring the system that hosts WACS involves the following tasks:

- *Creating a service account with delegation to be used for Vintela single sign-on* on page 46
- *Creating an SPN* on page 47
- *Resetting the service account password* on page 48
- *Creating and placing a keytab file* on page 48
- *Setting up multiple SPNs* on page 49
- *Increasing the header size limit of your WACS* on page 49

Creating 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 Active Directory on the Domain Controller.

To create a service account with delegation to be used for Vintela single sign-on, perform the following steps:

1. To register the service on the Domain Controller, open the **Active Directory Users and Computers** snap in.
2. Click the **Users** folder to view the list of users.
3. In the **Action** menu, click **New**, and then click **User**.
4. Type a name and a login name for the new service, and then click **Next**.

5. In the next screen, type a password for the service.

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

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

   This prevents the service account from expiring, which can 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 cannot view 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.
   - Currently, this service account cannot be set up with Microsoft's constrained delegation.

9. 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 then select **Use DES encryption types for this account**.

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

10. Click **OK**.

Creating an SPN

Note:
Make sure that the SPN you are creating does not 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 mapped to.

To create an SPN, perform the following steps:

1. Open a command prompt and navigate to your **Support Tools** folder.
2. Type 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 login name of the user account you created.

Resetting the service account password

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

To reset the service account password, perform the following steps:

1. On the Domain Controller with Active Directory installed, select **Start** > **Programs** > **Administrative Tools** > **Active Directory Users and Computers**.
2. Right-click the user account you created earlier, and click **Reset Password**.
3. Enter the new password in the New Password field
4. Re-enter the new password in the Confirm password field.
5. Ensure that **User must change password at next logon** is not selected.
6. click **OK**.

Creating and placing a keytab file

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

To create a keytab file, perform the following steps:

1. Run `ktpass` with the following arguments at the 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 you want to generate. (host.keytab, for example).
   - `HTTP/host@REALM` is the SPN created in *Creating an SPN* on page 47 (for example, HTTP/myurl.mydomain.com@MYDOMAIN.COM).
   - `user_password` is the password 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 *Creating a service account with delegation to be used for Vintela single sign-on* on page 46. 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 to the Java application system.

   Note:

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

Setting up multiple SPNs

Using multiple SPNs is not supported.

Increasing the header size limit of your WACS

Active Directory creates a Kerberos token that 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 WACS that hosts a Web Services SDK and QaaWS web service to use AD Kerberos single sign-on. Before you configure WACS, you must configure AD Kerberos single sign-on for the system that hosts the WACS.

To configure WACS for AD Kerberos single sign-on for Web Services SDK and QaaWS, perform the following steps:

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

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

Configuring Kerberos and single sign-on for the database

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

- SAP BusinessObjects Edge Series is deployed on WACS.
- WACS is configured with AD Kerberos.
- The database for 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 be 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 last step involves modifying the `krb5.ini` file to support single sign-on to the database.

Note:
If you want to configure end-to-end single sign-on for the database, you must also perform the configuration steps required for Vintela single sign-on. For information on configuring AD Kerberos single sign-on for Web Services

SDK and QaaWS, see *Configuring AD Kerberos single sign-on for Web Services SDK and QaaWS* on page 45.

Enabling single sign-on for the database

To enable single sign-on for the database, perform the following steps:

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

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

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

Configuring WACS in a complex environment

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

Using WACS with other web servers

Once a WACS is installed, it works as an application server and a web server without any extra configuration. You can configure the supported web servers such as Internet Information Services (IIS) and Apache to perform URL forwarding to the WACS server.

Note:
Forwarding requests from IIS to WACS by using an ISAPI filter is not supported.

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

Using WACS with a load balancer

To use WACS in deployment with hardware load balancer, you must configure the load balancer so that it uses either IP routing or active cookies. By configuring the load balancer, you ensure that after 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 that use passive cookies.

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

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

Related Topics

- *Configuring HTTPS/SSL* on page 15

Using WACS with a reverse proxy

You can use WACS in deployment that includes a forward or reverse proxy server. However, you cannot use WACS as a proxy server.

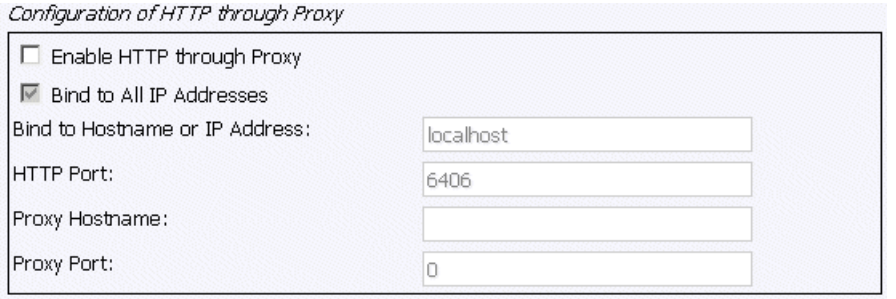
Configuring WACS to support HTTP with a reverse proxy

To use WACS in deployment that includes a reverse proxy, configure 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 outside the firewall (for example, the Internet).

To configure WACS to support HTTP with a reverse proxy, perform the following steps :

1. Navigate to the "Servers" management area of the CMC.
2. Double-click the WACS instance 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 HTTP port for WACS to use, to communicate through proxy.
   c. Specify Proxy Hostname and Proxy Port of the proxy server.



4. Click **Save & Close**.

Configuring WACS to support HTTPS with a reverse proxy

A few load balancers and reverse proxy servers can be configured to decrypt HTTPS traffic and 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 if you want to configure HTTPS with a reverse proxy, create two WACS instances. Configure one WACS instance for HTTPS for external traffic through the reverse proxy, and the other WACS instance 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 binds to all the IP addresses on the system that it is installed on. If you want 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.

For information about using a firewall between a WACS server and other SAP BusinessObjects Edge Series 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 WACS instance binds its HTTP port to all IP addresses. 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, perform the following steps:

1. Navigate to the "Servers" management area of the CMC.
2. Double-click the WACS instance 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 WACS to bind to.
4. In the "HTTPS Configuration" section, uncheck **Bind to all IP addresses**, and type an IP address or hostname for WACS to bind to.
5. Under "Common Settings", deselect **Auto assign**, and then specify the Hostname or IP Address of the NIC that is used for communication between WACS and the other SAP BusinessObjects Edge Series servers in your deployment.
6. Click **Save & Close**.
7. Right-click the WACS instance, and select **Restart Server** to restart the WACS instance.

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 3-1: General Properties

Property	Description	Range of Values
Log level	Specifies the minimum severity of warning that must be logged. The **DEBUG** level logs the maximum amount of activity, and the **FATAL** level 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 Time-out (seconds)	Specifies how long the WACS will wait for its hosted services to start before it times out. If the timeout passes, then 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 WACS does not start before time out, restore the default settings of the WACS through the Central Configuration Manager (CCM).	The default value is 300 seconds.

Table 3-2: 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 3-3: 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 3-4: HTTP Configuration Properties

Property	Description	Range of Values
Bind to All IP Addresses	Specifies 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 specify a value only 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 3-5: Configuration of HTTP through Proxy

Property	Description	Range of Values
Enable HTTP through Proxy	Specifies whether to enable HTTP through Proxy connector on WACS. This is typically checked in deployments with a reverse proxy.	True or False. The default value is False.
Bind to All IP Addresses	Specifies 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 specify a value only 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 specify a value only 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 specify a value only 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 specify a value only if you check **Enable HTTP through Proxy**.	Numeric values from 1 to 65535. By default, this value is empty.

Table 3-6: HTTPS Configuration

Property	Description	Range of Values
Enable HTTPS	Specifies 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 specify a value only 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 specify a value only 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 specify a value only 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 specify a value only 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 specify a value only 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 specify a value only 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 specify a value only 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.

Property	Description	Range of Values
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 specify a value only if you check **Enable HTTPS**.	The password for the private keys in your certificate stores.
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 specify a value only 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 can avail WACS services. Other clients are rejected. You can enable client authentication only if you check **Enable HTTPS**.	True or False. The default value is False.

Property	Description	Range of Values
Certificate Trust List File Location	The full name of the Certificate Trust List file. You can specify a value only 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 specify a value only 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 3-7: 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.

Property	Description	Range of Values
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 in 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.
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.

Troubleshooting

Viewing server errors

The log file is located at the *<InstallDir>*/Logging directory, where *<InstallDir>* is the path where SAP BusinessObjects Edge Series 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 when WACS was installed, *<timestarted>* is the time when 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.

Changing the logging level

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

Logging Level	Description
DEBUG	Logs all WACS activity. This option logs the maximum information. It is not recommended to select **DEBUG** in a production environment.
INFO	Logs general information. If you select **INFO**, the **WARN**, **ERROR**, and **FATAL** messages are logged to the log file.
WARN	Logs a message when the application encounters a problem. If you select **WARN**, the **ERROR** and **FATAL** messages are logged to the log file.

Logging Level	Description
ERROR	Logs a message when a service encounters an error or if a service is not available. If you select **ERROR**, the **FATAL** messages are logged 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 at the WACS command line. By default, this value is **ERROR**.

To change the logging level of a WACS, perform the following steps:

1. Navigate to the "Servers" management area of the CMC.
2. Double-click the WACS.

   Note:
   You need not stop the server.

   The "Properties" screen appears.
3. From the **Log Level** list, select a logging severity level, and click **OK**.
4. In the "Servers" screen, restart the WACS.

The logging level of WACS is modified.

Viewing system metrics

To view the system metrics of a WACS from the Central Management Console (CMC), perform the following steps:

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

The list of system metrics appears. For a description of the available metrics, see *WACS metrics*.

WACS metrics

The following table describes metrics that is displayed in the "Metrics" screen:

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

Viewing the state of a WACS

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

WACS supports a new server state called “Started with Errors”. If a WACS is in this state, then it indicates that WACS is running, but has at least one HTTP, HTTP through Proxy, or HTTPS connector that is not configured properly.

If the state of WACS status displayed as “Started with Errors”, navigate to the "Metrics" page and view the “"Running WACS Connector"” metric. If the enabled connectors do not appear in the list, then it indicates that the connectors have not been configured properly.

Resolving port conflicts

If you cannot view any pages when you attempt to access the CMC through a particular port, ensure that another application has not occupied 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 into the CMC and verify 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, then it indicates that these connectors are not able to start because of a port conflict.

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

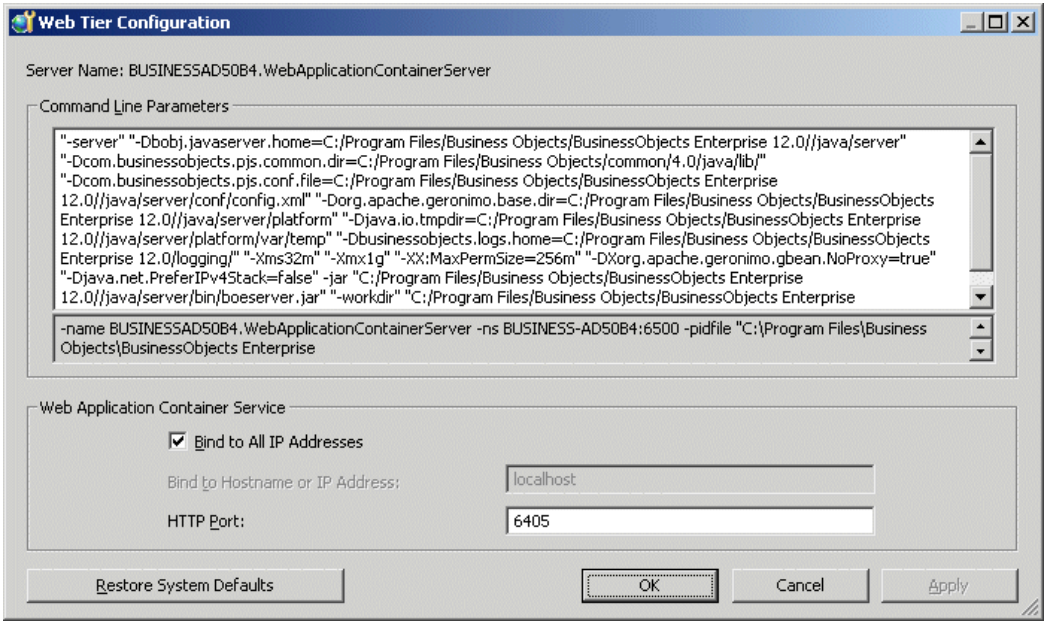
Resolving HTTP port conflicts

To resolve HTTP port conflicts, perform the following steps:

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

   Note:
   The **Web Tier Configuration** icon is enabled only when you select a WACS that is not running.

   The "Web Tier Configuration" screen appears.



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

Resolving HTTP through proxy or HTTPS port conflicts

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

To resolve HTTP through proxy or HTTPS port conflicts, perform the following steps:

1. Navigate 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**.

Changing the memory settings

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

To change the memory settings, perform the following steps:

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

   Note:
   The **Web Tier Configuration** icon is enabled only when you select a WACS that is not running.

   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 gigabyte of memory to the server.
   b. Specify a new value for the parameter.
      - To specify a value in megabytes, use “m”. For example, “-Xmx640m” allocates 640 megabytes of memory to the WACS.
      - To specify a value in giga bytes, use “g”. For example, “-Xmx2g” allocates two gigabytes of memory to the WACS.
   c. Click **OK**.
6. In the "Manage Servers" screen, start the WACS.

Changing the number of concurrent requests

The default number of concurrent HTTP requests that WACS is configured to handle is 150. This must 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 degrade performance. The ideal setting depends on your hardware, software, and IT requirements.

To change the number of concurrent HTTP requests, perform the following steps:

1. Navigate 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 required number of concurrent requests, and click **Save & Close**.
5. To start the WACS, right-click the server, and click **Start Server**.

Restoring default settings

If the WACS is not configured properly, you can restore the system defaults through the Central Configuration Manager (CCM).

To restore the default settings, perform the following steps:

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

   Note:
   The **Web Tier Configuration** icon is enabled only when you select a WACS that is not running.

The "Web Tier Configuration" screen appears.

5. Click **Restore System Defaults**.
6. If necessary, specify a free HTTP port, and click **OK**.
7. In the "Manage Servers" screen, start the WACS.

Preventing users from connecting to WACS through HTTP

In certain cases, you may want to allow users only 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 accepts only HTTP requests from the clients located on the same machine as the WACS. Following this method, you can perform maintenance or configuration tasks on the WACS through a browser on the same machine as the WACS, while preventing other users from accessing the server.

To prevent users from connecting to WACS through HTTP, perform the following steps:

1. Navigate 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 by using this method accepts connections from the local machine.

More Information

Information Resource	Location
SAP BusinessObjects product information	*http://www.sap.com*

Information Resource	Location
SAP Help Portal	Select *http://help.sap.com* > SAP BusinessObjects. You can access the most up-to-date documentation covering all SAP BusinessObjects products and their deployment at the SAP Help Portal. You can download PDF versions or installable HTML libraries. Certain guides are stored on the SAP Service Marketplace and are not available from the SAP Help Portal. These guides are listed on the Help Portal accompanied by a link to the SAP Service Marketplace. Customers with a maintenance agreement have an authorized user ID to access this site. To obtain an ID, contact your customer support representative.
SAP Service Marketplace	*http://service.sap.com/bosap-support* > Documentation • Installation guides: *https://service.sap.com/bosap-instguides* • Release notes: *http://service.sap.com/releasenotes* The SAP Service Marketplace stores certain installation guides, upgrade and migration guides, deployment guides, release notes and Supported Platforms documents. Customers with a maintenance agreement have an authorized user ID to access this site. Contact your customer support representative to obtain an ID. If you are redirected to the SAP Service Marketplace from the SAP Help Portal, use the menu in the navigation pane on the left to locate the category containing the documentation you want to access.
Developer resources	*https://boc.sdn.sap.com/* *https://www.sdn.sap.com/irj/sdn/businessobjects-sdklibrary*
SAP BusinessObjects articles on the SAP Community Network	*https://www.sdn.sap.com/irj/boc/businessobjects-articles* These articles were formerly known as technical papers.

Information Resource	Location
Notes	*https://service.sap.com/notes* These notes were formerly known as Knowledge Base articles.
Forums on the SAP Community Network	*https://www.sdn.sap.com/irj/scn/forums*
Training	*http://www.sap.com/services/education* From traditional classroom learning to targeted e-learning seminars, we can offer a training package to suit your learning needs and preferred learning style.
Online customer support	*http://service.sap.com/bosap-support* The SAP Support Portal contains information about Customer Support programs and services. It also has links to a wide range of technical information and downloads. Customers with a maintenance agreement have an authorized user ID to access this site. To obtain an ID, contact your customer support representative.
Consulting	*http://www.sap.com/services/bysubject/businessobjectsconsulting* Consultants can accompany you from the initial analysis stage to the delivery of your deployment project. Expertise is available in topics such as relational and multidimensional databases, connectivity, database design tools, and customized embedding technology.