Gentran Integration Suite™

WebDAV Server

Version 4.3

Sterling Commerce
An IBM Company

Contents

WebDAV Support in Application

Application supports the secure sending and receiving of files using the Web Distributed Authoring and Versioning (WebDAV) protocol.WebDAV is a standard extension to the HTTP/1.1 protocol that allows data to be written directly to WebDAV servers.

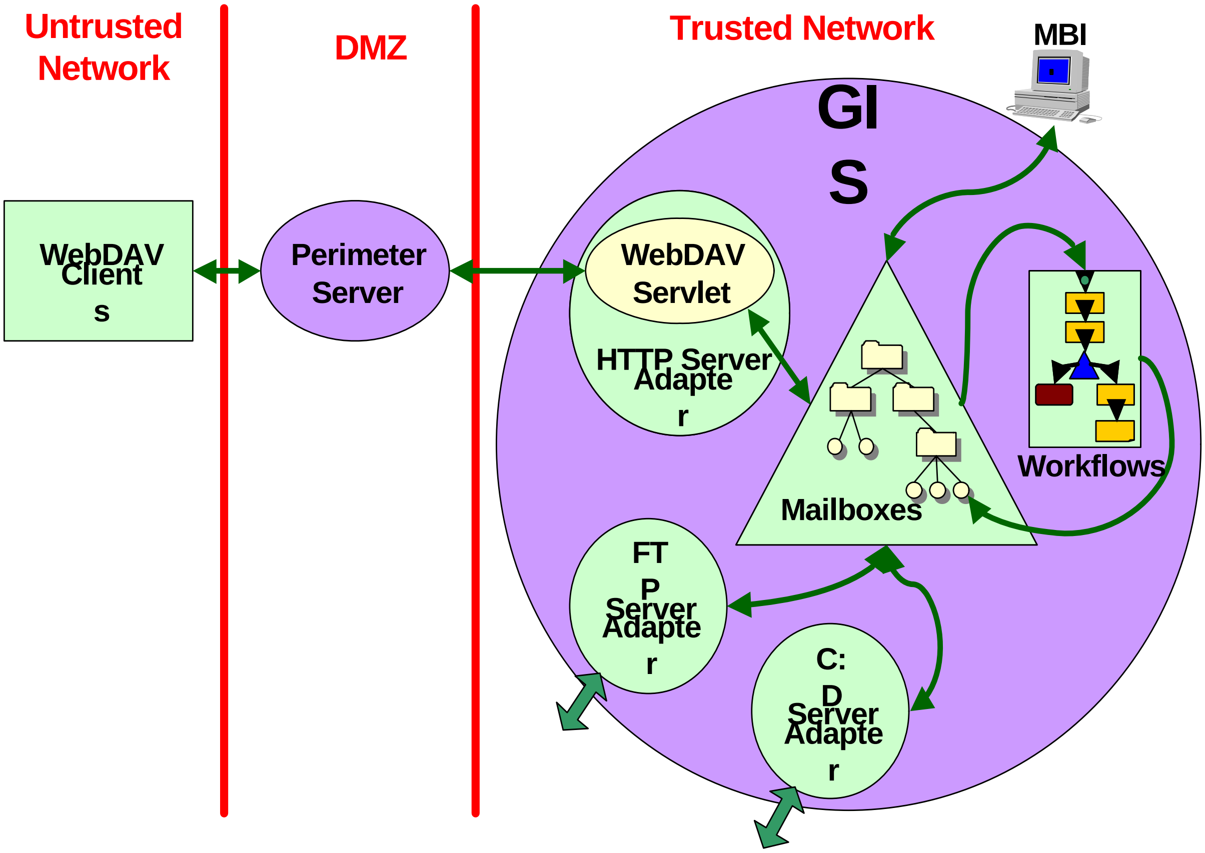
Windows XP integrates a WebDAV redirector into the file system. You can use any existing Windows application to access a WebDAV file share. Windows XP lets you use standard network UNC file format (that is, \\www.servername.com\target\dir\file.doc). In addition to the UNC format, when an application uses a standard Windows file dialog, it can also use the http: name format (that is, http://www.servername.com/target/dir/file.doc). This means you can open a file on the web, make changes, and if you have write permission, save it back.

While similar, WebDAV differs from the FTP protocol in that FTP uses two socket connections, one for data and one for control, while WebDAV uses a single connection. The advantage of using WebDAV is that it works through a firewall, as long as the firewall allows Internet HTTP traffic and does not explicitly filter out WebDAV packets. If you can browse the web, you can use WebDAV.

You can configure a WebDAV server within Application to send and receive files with trading partners using the following clients:

- Connect:Enterprise Secure Client
- Windows Explorer on Windows XP
- Any WebDAV client

The following figure shows how the WebDAV components integrate with Application:



Setting Up a WebDAV Server

To configure a WebDAV server for your Application system, perform the following tasks:

1. Set up a Mailbox in Application. Refer to *Using WebDAV with Application Mailboxes* on page 6.
2. Obtain and import system certificates. Refer to *Getting and Importing Certificates* on page 7.
3. Set up Perimeter Services. Refer to setting up perimeter services in the Application online library.
4. Configure and enable the HTTP Server adapter for WebDAV. *Setting up the HTTP Server Adapter for WebDAV* on page 10.
5. Edit the WebDAV properties file. Refer to *Editing the WebDAV Properties File* on page 11.
6. Provide connection information to your trading partners. You can use the worksheets in *Distributing WebDAV Server Information to Clients* on page 13 to distribute this information.

You are now ready to send and receive data with your trading partners who use WebDAV. Their data is handled the same as any other messages and documents in your Application Mailboxes.

Using WebDAV with Application Mailboxes

A *Mailbox* is a storage area for *messages*. Each message associates a name with some data (the data itself being stored in Application as a *document*.) Mailboxes are usually arranged in a hierarchy with the mailbox named / serving as the root.

Mailboxes in Application are analogous to the familiar directory structure offered by operating systems' file systems. A Mailbox is a directory and messages correspond to files in the directory.

Mailboxes are more feature rich than the normal file system. A mailbox can be configured to invoke a business process when a message is sent to it. Messages have well defined extractability policies that govern the conditions under which messages can be successfully extracted (opened.)

WebDAV is a protocol that defines a standard view of a repository that all WebDAV clients can uniformly access. The Application implementation of WebDAV uses Application Mailboxes as the repository. The prerequisites to using WebDAV in Application are:

- One or more Mailboxes setup as the repository for WebDAV
- Users with appropriate permissions to WebDAV Mailboxes

Setting up a Mailbox in Application on page 6

Setting up a User for Access to a Mailbox on page 7

Setting the Mailbox Properties File on page 7

Setting up a Mailbox in Application

Create a Mailbox for a specific trading partner if each trading partner should see only their own data. It is convenient if the mailbox is named so that the associated trading partner can be discerned from the mailbox name.

To create a mailbox in Application:

1. In the Admin console, select **Deployment** > **Mailboxes** > **Configuration**.
2. In the Create section, click **Go!**
3. Complete the Name page as described in the following table, then click **Next**.

In this field	Type or select	Description
Parent Mailbox	/	The root mailbox is denoted by a slash (/). Required.
Name	*mailbox_name*	This name identifies the mailbox in Application. Required.
Description	*WebDAV repository*	Use this field to describe the mailbox. This field is not used by any other resource in the system. Required.

4. Click **Next** in the Assign Groups page.

5. Click **Next** in the Assign Users page.
6. In the Confirm page, review the information and click **Finish**.
7. Click **Return**.

Setting up a User for Access to a Mailbox

Before your trading partners can access your Application from a WebDAV client, your administrator must add a user account for them with the right permissions. In the case of a WebDAV client, these permissions include access to one or more Application Mailboxes that you set up exclusively for them. A user account is comprised of a user ID and password.

Setting the Mailbox Properties File

Set the following value in your mailbox.properties file:

```
disallowDuplicateMessages=true
```

This ensures that every message in a single mailbox has a unique name. It also ensures that a message and a mailbox do not have the same name. If you write a message to a mailbox and the name matches the name of a message in the mailbox, the old message is deleted before the new message is added.

Getting and Importing Certificates

A System Certificate is comprised of two related cryptographic entities, a private key and a public certificate. Public key cryptography is the technology that grants the possessor of the private key the exclusive ability to decrypt messages encrypted with the corresponding public certificate (which contains the public key certified by a trusted, third party certificate authority.)

It is imperative that the private key be a closely guarded secret as any possessor of the private key can access encrypted messages that were intended to be confidential.

Public key cryptography can be used for authentication. By proving that they own the private key without disclosing it, a party irrefutably proves their identity.

- ✦ *Generating Private Keys* on page 7
- ✦ *Obtaining Public Certificates* on page 9
- ✦ *Generating a Keycert File* on page 9
- ✦ *Importing System Certificates into Application* on page 9

Generating Private Keys

Use the Sterling Commerce Certificate Wizard in Application to create a system certificate:

1. From the Application Admin Console, select **Trading Partners** > **Digital Certificates** > **System**.

2. At **Run Certificate Wizard**, click **Go!** If this is the first time to run the Certificate Wizard, click **download Java Web Start**. Follow the instructions to install and then click **Go!** to start the Certificate Wizard.
3. When Java Web Start issues its warning that the application (Certificate Wizard) is requesting unrestricted access to the file system and the network, verify that the dialog includes the following:

   Signed and distributed by: Sterling Commerce America

   Publisher authenticity verified by: VeriSign, Inc.
4. Click **Start**.
5. Select **Certificate Request**. Use the following table to complete the fields:

Field	Description
Common Name	Domain name of the system that Application Perimeter server is installed on, as published to WebDAV and HTTP clients. Required. **Note:** If access is through a firewall and NAT (Network Address Translation), the Common Name must match the host name that clients connect to. **Note:** The port number must not be included in the Common Name.
Country	Country where the server is located. Required.
State/Province	State or Province where the server is located. Required.
City/Locality	City or Locality where the server is located. Required.
Organization/Company Name	Organization or Company Name that owns or administers the server. Required.
Organizational Unit	Organizational unit that owns or administers the server. Required.

6. Click **Next** to generate a private key. Type random keystrokes until a dialog indicates that a suitable level of randomness has been collected. Click **OK**.
7. Choose a suitable length for the private key to be generated. Valid values are:
   - 512
   - 768
   - 1024
   - 2048

   In general, messages encrypted with longer keys are harder to break than those encrypted with shorter keys and they remain secure for a longer period of time. The downside to using longer keys is that encryption and decryption take longer and negatively affect performance. Also, clients may only support a particular key size.
8. Complete and confirm a passphrase. Choose a string between 6 and 255 characters.

   Anytime the private key must be used, the passphrase must be supplied with it.If the passphrase is lost, it cannot be recovered from the private key or from any other file.
9. Click **Next**.
10. Complete the following fields and browse to a directory to store the files:

- Private key file name
- Certificate Signing Request (CSR) file name

11. Click **Finish**.
12. Copy the resulting key. Send the public key to the certificate authority (CA), packaged as a CSR using whatever mechanism and process specified by your CA.

Note: The CSR does not contain the private key. The CA has sufficient information to issue or deny a certificate based on the CSR. A CA should not need to ask for your private key.

Obtaining Public Certificates

Purchase a public certificate only from a reputed certificate authorities. Copy the certificate (all lines between and including -----BEGIN CERTIFICATE----- and -----END CERTIFICATE-----) into a file on your disk.

Root certificates from many well-known certificate authorities are preinstalled with Windows XP and do not require a manual step by the users of the clients.

Generating a Keycert File

Now you are ready to concatenate the encrypted private key and the certificate authority issued certificate into a single keycert file. To generate a keycert file:

1. Select **Generate Keycert**. Enter the locations of the private key file and the digital certificate file and the destination for the keycert file.
2. Click **Generate**.
3. Select **Verify Certificate** and click **Verify**.

Importing System Certificates into Application

The System Certificate is the combination of the public root certificate from the CA and the private key.

Now you are ready to import the public root certificate of the CA into the CA Certificates repository in Application. Download the root certificate from the CA's website and save as a file on the local system where the web browser runs.

To import this root certificate file into Application:

1. Select **Trading Partner > Digital Certificates > CA**. Click the **Go!** next to **Check in New Certificate**. Application accepts certificates in the DER and the Base64 formats. Certificate files in the DER format usually carry a .cer or .der file name extension.
2. Click **Next**. Certificate Name contains a name fabricated by the CA and the serial number but you can replace this with a more readily apparent name.
3. Verify that the **Status** is **Verified.** Click **Next**. Check **Validate When Used**.
4. Click **Next**. Click **Finished** on the summary page to complete the import of the CA certificate.

Now you are ready to import the Key Certificate into Application. To import the Key Certificate:

1. From the Admin Console, select **Trading Partner** > **Digital Certificates** > **System**.
2. Click the **Go!** next to **Check in Key Certificate**. Complete the fields with a convenient name for the certificate, the keycert file generated by Certificate Wizard, and the passphrase for the keycert file.
3. Click **Next**.
4. Select the options based on the following descriptions and click Next:

Field	Description
Validity	Controls whether the system certificate must be revalidated each time it is used
Auth Chain	Controls whether the certificate chain up to the root CA certificate must be revalidated each time the certificate itself is revalidated
CRL cache	Controls whether the CRL Cache is consulted each time the system certificate is used

Setting up Perimeter Services in Application

A perimeter server is communications management software that is installed in a DMZ of a company network. A perimeter server and its client manage communication flow between the perimeter network and the Application adapters. To use WebDAV to send and receive data from external trading partners, you must set up perimeter services. Refer to setting up perimeter services in the Application online library for complete details and procedures.

Setting up the HTTP Server Adapter for WebDAV

The HTTP Server adapter handles incoming WebDAV requests, while leveraging the Perimeter Services infrastructure. Specify what happens to an arriving WebDAV request in one of two ways:

- Configure a URI on the adapter so that when requests arrive at that URI, a business process is invoked.
- Set up a URI so that the adapter delegates to a web application bundled as a Web Application Archive (WAR) file.

Application supports WebDAV through use of a WAR file. The webdav.war file is part of the standard Application installation and is usable when the WebDAV feature is licensed.

HTTP clients need to know the HTTP Server adapter configuration, the host, port, and URI (URL) to send requests to. The host that clients connect to is the Perimeter server. The HTTP listen port and Perimeter server internal port must be different.

Configure the HTTP Server adapter basic authentication for initial security and for SSL for additional security. Basic authentication prompts users for their user ID and password defined in Application.

To configure the HTTP Server adapter:

1. From the **Admin Console, select Deployment > Services > Configuration**. Click **Go!** next to **Create New Service**.
2. For the Service Type, enter **HTTP Server adapter** or select from a list of available service types. Do not use the B2B HTTP Server adapter. Click **Next**.
3. Enter a unique name and description. The **Select a group** value can be left at the default of **None**. Click **Next**.
4. On the **HTTP Connection Properties** page, enter the HTTP listen port and choose from the list of Perimeter server names the one previously configured.
5. Set **User Authentication Required** to **Yes**.
6. **Set Use SSL** to **Must**. Click **Next**.
7. On the SSL Settings page, for the **System Certificate** choose the previously imported system certificate generated with Certificate Wizard.
8. Set the **Cipher Strength** to **STRONG**.
9. Leave the **CA Certificate** selections list (on the right) empty.
10. Click **Next**.
11. Click **add** and enter the URI for the webdav.war file in the Application installation directory. Choose **War File** on the **URI Config** page.
12. On the WAR Config page, append '/noapp/deploy/webdav.war' to the Application installation directory to derive the absolute path to this particular war file.

    Specify the absolute path to the war file on the system on which Application is installed (not the system that runs the web browser.)

    If the war file does not exist as specified by the path, you will return to the URI Config page.
13. Click **Next**. Click **Finish** to complete the adapter configuration process.
14. Use the netstat command on the Perimeter server system to verify that the HTTP listen port is connected.

Editing the WebDAV Properties File

The WebDAV properties file is where you set the following values:

Property	Description and Values
Storage type	How new documents are stored. Valid values are: ◆ default - use the system default ◆ db - store documents in a database ◆ file - store documents in file system

Property	Description and Values
Extractable	Extractability to use for new documents. Valid values are: ◆ yes - document is always extractable ◆ no - document is never extractable ◆ count - document is extractable for the specified count* ◆ time - document is extractable for the specified time* Default is extractable=yes. *requires additional parameters
Extractablecount	Number of times document is extractable if extractible=count. Default is 1. Example: Document is extractable five times. Properties file includes: ◆ extractable=count ◆ extractablecount=5
Extractabledays	Number of days document is extractable if extractable=time. Default is 0. Example: Document is extractable for one day. Properties file includes: ◆ extractable=time ◆ extractabledays=1
Extractablehours	Number of hours document is extractable if extractable=time. Default is 0. Example: Document is extractable for 1 day, 5 hours, and 34 minutes. Properties file includes: ◆ extractable=time ◆ extractabledays=1 ◆ extractablehours=5 ◆ extractableminutes=34
Extractableminutes	Number of minutes document is extractable if extractable=time. Default is 0. Example: Document is extractable for 1000 minutes.Properties file includes: ◆ extractable=time ◆ extractableminutes=1000

Use a text editor to edit the properties file.The following is a sample webdav.properties file:

```
storagetype=default
extractable=yes
```

Distributing WebDAV Server Information to Clients

Use the following worksheet to inform your trading partners how to connect to your server using WebDAV. When you distribute this information, refer the trading partner to the Application WebDAV Client Guide.

Worksheet for a WebDAV Server
Fully qualified host name (host name and domain name) or IP address of server:
HTTPS port number:
Connection URL path:
User ID:
Password:
Trusted root certificate or direct trust certificate for Secure Sockets Layer protocol:
Is this certificate preinstalled in Windows XP?
Does server require SSL client authentication?
What cipher suites does this server use?

Known Restrictions for WebDAV Servers

Application WebDAV Client has the following restrictions:

- A new folder cannot be created in this WebDAV network place by the client. Instead, the Application administrator must create a new mailbox (with the current mailbox as the parent) and give the appropriate users permissions to that mailbox.
- A file cannot be deleted from a WebDAV folder.
- A file in a WebDAV folder cannot be renamed.
- Conventional file locking that applications (such as Microsoft Word and Excel) perform on folders to ensure safe concurrent usage of a document do not work. Some applications, such as Microsoft Word, continue to work as if the lock has been acquired when it has not been.
- When a Application message ceases to be extractable anymore (as determined by the extractability policy) the corresponding file will show up in the network place but one will get errors trying to access it.
- The WebDAV client built into Windows and accessed through Network Places keeps an internal copy of credentials given to it. It is unknown how long Windows keeps these credentials or when you can replace them. Restarting Application does not affect this Windows credential cache.
- Only one level of listing is supported for PROPFIND.
- The HTTP Server adapter only allows messages smaller than 2GB to be sent to the HTTP server from the client.

Index