Setting Up Groupware Integration

deem

deem.com

Why Integrate with Groupware?

You can integrate Deem services such as booking travel and arranging for shipping with your groupware calendars and contacts. For example, as a user books travel, the service can automatically update enterprise or personal calendars with reservation details and changes. And if a travel delegate (arranger) books a trip for someone else, the trip information automatically appears on that person's calendar.

This convenience provides the following benefits:

- Eliminates the need for the user to manually enter and maintain reservation information.
- Ensures that the details are always immediately accessible.
- Users with calendars on their smartphones don't have to print out the information.
- Updates happen automatically.
- Saves time for a travel delegate or arranger who books a trip for someone else by eliminating the copying and pasting into the traveler's calendar.

Choosing an Integration Type

You can integrate with existing enterprise groupware solutions such as Microsoft Exchange, IBM (Lotus) Domino, and the calendar in Google Services, and also with personal calendar and address book solutions such as Google Calendar, Apple Calendar (formerly iCal), Yahoo, and Microsoft Outlook. There are two ways to integrate with groupware:

Inline and iCalendar Attachment Integration:
With Inline and iCalendar Attachment integration, the Notification Service sends emails with invitations or attached appointments. For details on how to enable this type of integration, see **Inline and iCalendar Attachment Integration**.

Enterprise and Personal Groupware Integration:
These configurations offer tighter integration for automatically populating calendars with appointments. Establishing integration at an enterprise level may require downloading and installing utilities and changing groupware configuration settings. We offer the following integration choices:

- **Enterprise Groupware with Microsoft Exchange**
- **Enterprise Groupware with IBM (Lotus) Domino**
- **Enterprise Groupware with Google Services**
- **Personal Synchronization with Google Calendar**
- **Feed with Personal Calendars**

In addition to these pages, we can provide more information and help you with your integration. Send us an email at integration@deem.com.

Security

Deem takes the security of your groupware systems very seriously and built a tiered security mechanism to ensure that security is not compromised. To enable enterprise integration, Deem uses XML-based web services to create, update, and delete calendar entries on behalf of users. These operations are performed using a minimal permission delegate account, ensuring that Deem never has access to user account credentials. The services themselves are comprehensively secured through both message authentication and transport security.

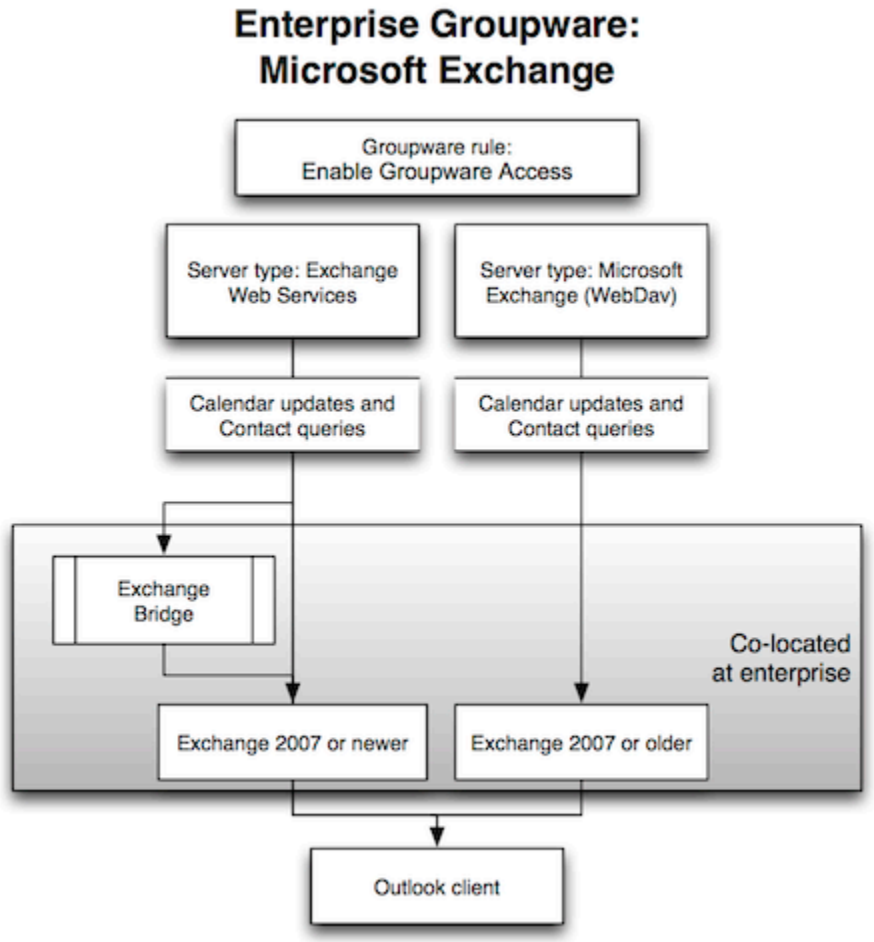
Enterprise Groupware with Microsoft Exchange

deem.com

Overview

Deem integrates with Microsoft Exchange 2003, 2007, 2010, and 2013, using both forms-based and standard login authentication. It requires an Outlook Web Access (OWA) server. Travel and other services integrate with Exchange by logging in as a limited rights delegate account through the OWA interface using WebDav (Web-based Distributed Authoring and Versioning) over the SSL protocol, or using Exchange Web Services. As a result, calendar events are automatically added to the user's calendar as the user books travel, and contact information appears for quickly selecting an invitee or recipient of a service.

The following diagram illustrates how this integration works:



All communication is performed over SSL, ensuring that messages are not viewed or tampered with in transit. This is the same interface that is used and exposed for Outlook Web Access, and hence leverages the native security of that platform.

Deem uses a minimal permissions delegate account when performing groupware operations. This account only has permissions to create, update, and delete Deem-related calendar entries. This ensures that the user's credentials are not required and never exposed. These credentials can be input directly by customer IT staff, and are encrypted both by the application, as well as the database to ensure secure storage. The delegate requires minimally invasive "Author Access" to user calendars. This allows for create, edit, and delete permissions only for calendar items that are authored by the delegate, *not* for other items. In addition, the delegate gets "Reviewer" read-only access for contact lookups. The delegate account can't update any user credentials.

Enabling Enterprise Groupware with Exchange

Note: Enterprise Groupware with Microsoft Exchange is a Premium Service and requires a separate agreement with Deem to be in place before configuration can take place. If you are unsure if your agency has this service included in your reseller agreement with Deem, please enter a support case (see Entering a Support Case for instructions).

Choose **Exchange Web Services** as the server type for Exchange 2007 or newer, or **Microsoft Exchange (WebDav)** as the server type for Exchange 2007 or older. Users access Exchange through their Outlook client application. This integration method offers calendar updates and can also be optionally configured for contact queries.

For instructions on setting up Microsoft Exchange integration, see **Microsoft Exchange Setup**.

Frequently Asked Questions (FAQs)

Our security protocols do not allow for the installation of 3rd party applications to be installed on our hardware. Can the permissions be applied without the use of the 3rd party application?

We do not provide support for any other means of applying the delegate permissions; therefore it is recommended that the Delegate Utility be utilized when applying the delegate permissions to the end users. You are however free to use your own method, as long as all of the appropriate permissions are set.

With regards to the "delegate account", does this account require any special permissions?

The delegate account is a permanent account, and is just a regular mail account (e.g. not an admin or with any other special powers). The delegate account must be able to send e-mail as well as receive e-mail from an external source. Make sure that the delegate account has a non-expiring password.

We have multiple Exchange servers. Is calendar/contact integration able to work with multiple Exchange servers?

Yes, however we need to have a means to differentiate the users on each Exchange server. Please work with your Deem integration manager to ensure the users can be differentiated.

If a calendar event fails to write to a user's calendar, is there a retry mechanism present?

A mechanism is in place that makes three additional attempts to write to the user's calendar. If there is a failure, the system calculates the delay between the moment of failure and the start time for the event. If this delay is greater than 36 hours, a retry is scheduled for 24 hours after the moment of failure. If the delay is less than or equal to 36 hours, the retry is scheduled for half of the difference between the moment of failure and the start time for the event, up to a maximum of 18 hours after the moment of failure. If the retry fails, the system calculates the delay between the moment of the retry failure and the start time for the event, and uses the same algorithm to schedule another retry. If the second retry fails, the system uses the same calculation and algorithm to schedule a third retry. Each actual retry occurs soon after the schedule for the retry.

Microsoft Exchange Setup

Overview

The following versions of Microsoft Exchange are supported for full calendar and contact integration using forms based and standard authentication to Outlook Web Access (OWA):

- Exchange 2003 (SP2 or higher): Using the WebDAV protocol, authenticating as the delegate account, through your externally available OWA (Webmail) interface.
- Exchange 2007: Using the WebDAV protocol or Exchange Web Services, authenticating as the delegate account, through your externally available OWA (Webmail) interface or your Exchange Web Services URL.
- Exchange 2010 and 2013: Using Exchange Web Services, authenticating as the delegate account, through your externally available Exchange Web Services URL.

For versions of Microsoft Exchange other than those listed above, contact integration@deem.com for more information.

Due to Microsoft limitations, we suggest that if you are using Exchange 2010, *all* travelers should be migrated to an Exchange 2010 Server. Calendar Groupware does not work cohesively between Exchange 2010 and earlier versions of Exchange.

Setting Up Exchange

Outlook Web Access or Exchange Web Services must be deployed and available from the Internet.

Follow these steps to set up Microsoft Exchange:

1. Create the Delegate Account.
   Click here to expand...

   Microsoft Exchange integration needs a delegate username and password, which is used to access the user calendar. The delegate account is a regular email account, not an admin account. This is the account that is used for all groupware interaction and has just enough permission to perform calendar and contact integration. The delegate is able to create new events on users' calendars, but can only modify or delete events it has created. The delegate is able to access a user's personal contacts (if the contact list is on the server) in order to display them within the service, but cannot change them.

   The delegate account should be visible in the system (we suggest you use the name "Deem Delegate").

   Warning: If the account's password expires, the Exchange integration will not work. Create a non-expiring account.

   Your Delivery Manager will need the delegate account credentials prior to obtaining the permission management utility for you. Communicate the delegate account's username and password to the Delivery Manager in a secure manner:

   - Send the username as part of Data Collection Form in Step 2 (the next step).
   - Send the password in a separate email to integration@deem.com or send a request to contact you to communicate the password over the phone. The password is masked and encrypted in our system.

   The delegate will have access to the Access Control List which will have the following attributes enabled:

   - Create documents
   - Delete documents
   - Read public documents
   - Write public documents
   - Replicate or copy documents

   Note: The customer's IT department has full control of the delegate password. The delegate password is encrypted and stored securely. Deem uses XML-based web services to create, update, and delete calendar entries on behalf of users. These operations are performed using a minimal permission delegate account, ensuring that Deem never has access to end-user account credentials. The services themselves are comprehensively secured through both message authentication and transport security.

   Contact your Deem Delivery Manager or email us at integration@deem.com for more information on the Delegate Utility.

2. Complete the Data Collection Form (click to download the form). Once completed, email to integration@deem.com.
3. Configure and validate permissions.
   Click here to expand...

   Permissions need to be assigned to all users who have calendar integration. You will need to create a process for ensuring new users receive the appropriate permissions.

   The delegate account must be given permission to review each user's personal contacts, and to add, modify, or delete calendar events that the delegate account created. Deem provides the Delegate Utility to help manage this process for large user populations.

   To validate your configuration, your Deem Delivery Manager needs detailed information about your server, the delegate account you wish to use, and the name of the test account you'd like to validate. Please work with your Delivery Manager to provide the required information.

   Deem can then work to complete the configuration of the site and will work with you to run some simple tests to validate that your Exchange integration is configured properly.

4. Assign permissions manually or using the Delegate Utility.
   Click here to expand...

   You can use the Delegate Utility to set the appropriate permissions for a large groups of users. Use the links below to read the instructions and download the utility.

   Once you have validated your configuration, you need to rerun the Delegate Utility to establish permission all users who use the Deem services. This step completes the integration; however, you may want to run the Delegate Utility to add new users.

   Using the Delegate Utility for Exchange 2003 or 2007

   Using the Delegate Utility for Exchange 2007 or 2010

Enabling the Groupware Server in the Partner Dashboard

The Deem Activations team or your system administrator enables enterprise groupware in the Partner Dashboard by following these steps:

1. Log into the Partner Dashboard as the site administrator.
2. Click the **Groupware Servers** link under the Settings tab.
3. Click the **Add Server** link to show the Add Server page and add a server, or click the link for an existing groupware server to show the Edit Server page and edit the server's settings.
4. If adding a server, enter a Server or Gateway name for easy identification when choosing servers for groups.
5. Choose the server type from the Server Type drop-down menu. The server type should be one of the following:
   - **Microsoft Exchange (WebDav)** for enterprise integration with Microsoft Exchange 2007 or older.
   - **Exchange Web Services** for enterprise integration with Microsoft Exchange 2007 or newer.
6. Enter or choose additional parameters depending on the choice in the previous step, based on the information in the Data Collection Form. For example, you may need to enter the Delegate User mailbox ID and its password.
7. (Optional) You can also enter a Groupware ID in the Groupware ID field, or click the option to use the fully qualified email address as the Groupware ID. This value is used for testing purposes only.
8. Click the **Save** button to save the server settings.
9. To commit these changes, click the green **Changes not applied** link in the top right corner of the page, and then click the **Commit** button .

Assigning the Groupware Rule to a Group

To assign the groupware rule to the group, follow these steps:

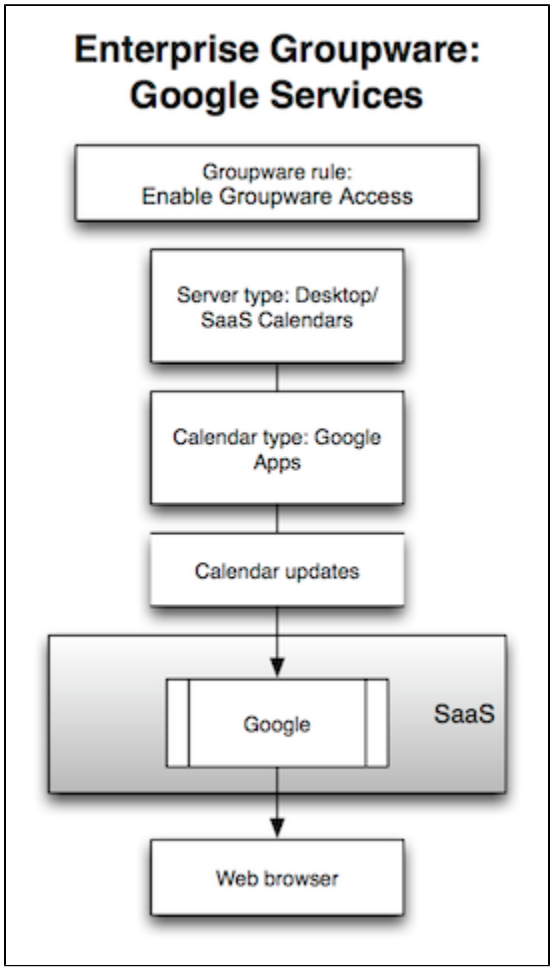
1. Log into the Partner Dashboard as the site administrator.
2. Click the **Rules** tab, and then click the **Groupware Rules** link.
3. Click the **Add** button next to the group name (or the Everyone group).
4. Enter a Rule Description that describes the intent of this rule, and click the Activate Rule checkbox.
5. Scroll down to the "Then" section of the page, and click the "Enable groupware access" checkbox.
6. Select the server or gateway name (the name you entered in Step 4 in the previous steps for adding the groupware server) from the Use Groupware Server drop-down menu, and click the "Enable calendar updates on this server" and "Enable address book lookups on this server" checkboxes.
7. Click the **Save** button to save the settings.
8. To commit these changes, click the **Changes not applied** link in the top right corner of the page, and then click the **Commit** button.

Enterprise Groupware with Google Services

deem.com

Overview

Deem can integrate with Google Services at the enterprise level, as shown below:



The Desktop/SaaS Calendars server type provides enterprise integration with Google Services. Users access Google Services through their web browser. This integration method offers only calendar updates; integration with contacts or address books is not supported.

For instructions on enterprise groupware with Google Services, see **Google Services Setup**.

Google Services Setup

Google Services integration setup is performed by the site administrator in the Partner Dashboard.

Overview

Note: If you previously set up Google Services integration, you may have to reconfigure Google's Admin Console. Google Services integration for the enterprise has been upgraded to use the newest Google calendar features and application programming interface (API). As a result, you need to configure Google's Admin Console to allow the new Google "OAuth2" token.

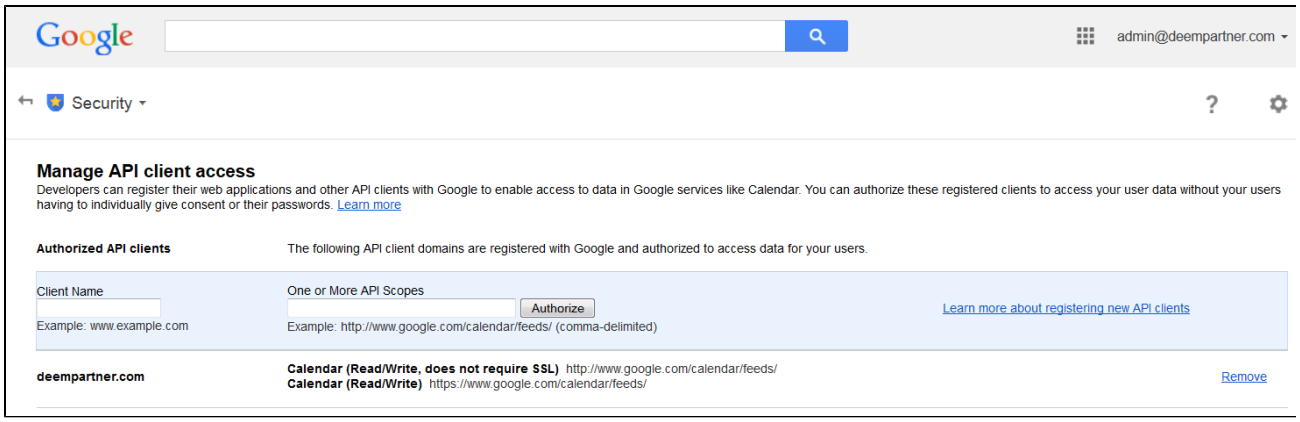
Tip: Trip modifications may not appear in the Google calendar for trips booked previously.

To enable enterprise groupware with Google Services, you must configure Google's Admin Console to enable "OAuth2" token access. You then enable the groupware server and provide its settings by logging into the Partner Dashboard as the administrator, and choosing **Desktop/SaaS Calendars** as the server type.

Enabling Access

Follow these steps to configure Google's Admin Console:

1. Sign into the Google Admin Console (admin.google.com) as an administrator, and click **Security**.
2. Click **Show More**, click **Advanced Settings**, and then click **Manage API client access**. The Manage API client access screen appears, as shown below, with your current configuration (shown as "deempartner.com") at the bottom of the "Authorized API clients" section:



3. Enter the following into the Client Name field of the "Authorized API clients" section (you can copy and paste the text):

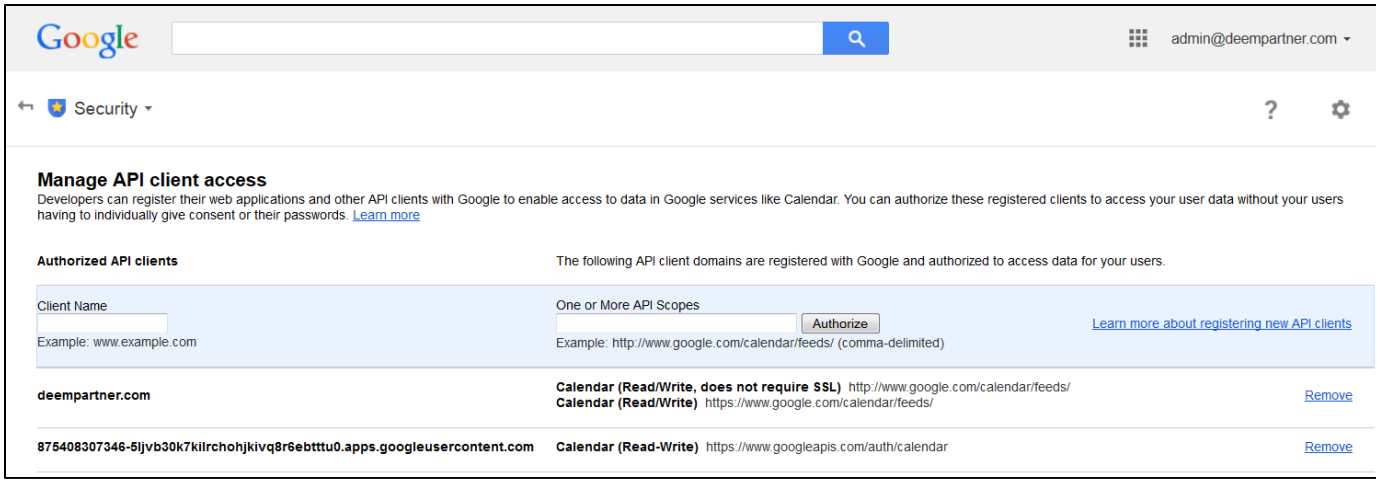
   875408307346-5ljvb30k7kilrchohjkivq8r6ebtttu0.apps.googleusercontent.com

4. Enter the following into the "One or More API Scopes field of the "Authorized API clients" section (you can copy and paste the text):

   https://www.googleapis.com/auth/calendar

5. Click the **Authorize** button.

Your new configuration now appears below the previous configuration:



Enabling the Groupware Server in the Partner Dashboard

The Deem Activations team or your system administrator enables enterprise groupware in the Partner Dashboard by following these steps:

1. Log into the Partner Dashboard as the site administrator.
2. Click the **Groupware Servers** link under the Settings tab.
3. Click the **Add Server** link to show the Add Server page and add a server, or click the link for an existing groupware server to show the Edit Server page and edit the server's settings.
4. If adding a server, enter a Server or Gateway name for easy identification when choosing servers for groups.
5. Choose the server type for Google Services from the Server Type drop-down menu: **Desktop/SaaS Calendars**.
6. Choose the calendar type for Google Services in the Calendar Type drop-down menu: **Google Apps**.
7. Select either **Use Dedicated Calendar** or **Use Primary Calendar** for the Calendar Choice. If you choose Use Dedicated Calendar, you must then enter the Google Calendar name and pick a Google Calendar Initial Color. The name and color correspond to the name and color of the calendar within Google Calendar that you want to use for your travel information.
8. (Optional) You can also enter a Groupware ID in the Groupware ID field. This value is used for testing purposes only.
9. Click the **Save** button to save the server settings.
10. To commit these changes, click the green **Changes not applied** link in the top right corner of the page, and then click the **Commit** button .

As part of the process, we would like to test users to assure that the Google Apps Connectivity is working correctly. Please email integration@deem.com with one email addresses that we can test to make sure we are able to connect to the Google Apps calendar correctly.

Assigning the Groupware Rule to a Group

To assign the groupware rule to the group, follow these steps:

1. Log into the Partner Dashboard as the site administrator.
2. Click the **Rules** tab, and then click the **Groupware Rules** link.
3. Click the **Add** button next to the group name (or the Everyone group).
4. Enter a Rule Description that describes the intent of this rule, and click the Activate Rule checkbox.
5. Scroll down to the "Then" section of the page, and click the "Enable groupware access" checkbox.
6. Select the server or gateway name (the name you entered in Step 4 in the previous steps for adding the groupware server) from the Use Groupware Server drop-down menu, and click the "Enable calendar updates on this server" and "Enable address book lookups on this server" checkboxes.
7. Click the **Save** button to save the settings.
8. To commit these changes, click the **Changes not applied** link in the top right corner of the page, and then click the **Commit** button.

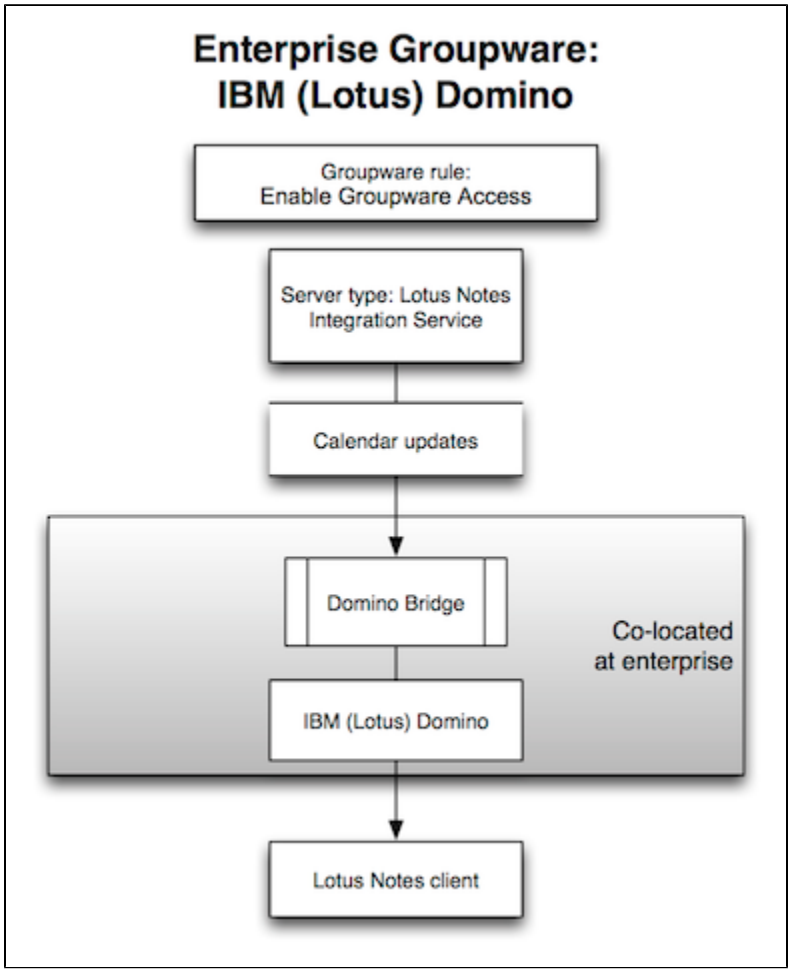
Enterprise Groupware with IBM (Lotus) Domino

deem.com

Overview

Deem can establish integration at the enterprise level with IBM (Lotus) Domino – versions R8.5.x and R9.0.x. Choose **Lotus Notes Integration Service** as the server type (for Domino Bridge) in the Partner Dashboard.

Users access Domino through their Lotus Notes client app. This integration method offers only calendar updates; integration with contacts or address books is not supported.



Lotus Notes integration requires deploying a small web application that accepts secure SOAP requests (over SSL) and translates these into calendar events. The web application uses a minimal-access delegate account to connect over DIIOP to your Domino server and create calendar entries on behalf of users. Additionally, each message is authenticated with a dedicated service account. Account credentials are never sent with the message. Rather, a keyed-Hash Message Authentication Code (HMAC) is used, along with time-stamp based message replay protection. This combination of techniques creates a message exchange pattern that is extremely secure. The web application also uses the same technique to modify or delete calendar entries that it had created.

The integration uses a minimal permissions delegate account to perform groupware operations. The delegate account password is stored with the web service on your infrastructure, and is encrypted using AES 128-bit encryption. Deem uses a service password you select to communicate with the web service. No delegate credentials are stored within the Deem system.

Deem uses a minimal permissions delegate account when performing groupware operations. This account only has permissions to create, update, and delete Deem-related calendar entries. This ensures that the user's credentials are not required and never exposed. The delegate

requires minimally invasive “Author Access” to user calendars. This allows for create, edit, and delete permissions only for calendar items that are authored by the delegate, *not* for other items. In addition, the delegate gets the least invasive setting, “No Access” with read-write access only to public documents. The delegate account can't update any user credentials.

For instructions on setting up Lotus Notes integration, see **Lotus Notes Setup**.

Frequently Asked Questions (FAQs)

Does the web app need to be installed on our Domino server?

The web application does not need to be installed on the Domino server. However it needs to be installed in a location that can talk to the server where the delegate user resides. That Domino server must also have DIIOP enabled.

We have multiple Domino mail servers. How do you manage the update of a user's calendar who is located on a mail server other than the specified mail server in the configuration of the web server?

The WAR file is deployed to talk to the server that has DIIOP enabled. From there, this "Gateway Server" has the directory containing all users and the server the reside. When the Deem service makes a calendar entry request, our request via DIIOP first looks up the user against the Domino directory based on Groupware ID that we have (typically the email address). The Domino directory knows on which server the user is and from that point on, native Domino calls route the calendar entry to the appropriate server.

If a calendar event fails to write to a user's calendar, is there a retry mechanism present?

A mechanism is in place that makes three additional attempts to write to the user's calendar. If there is a failure, the system calculates the delay between the moment of failure and the start time for the event. If this delay is greater than 36 hours, a retry is scheduled for 24 hours after the moment of failure. If the delay is less than or equal to 36 hours, the retry is scheduled for half of the difference between the moment of failure and the start time for the event, up to a maximum of 18 hours after the moment of failure. If the retry fails, the system calculates the delay between the moment of the retry failure and the start time for the event, and uses the same algorithm to schedule another retry. If the second retry fails, the system uses the same calculation and algorithm to schedule a third retry. Each actual retry occurs soon after the schedule for the retry.

What application servers does the Web Application work on?

The Lotus Integration web application will work with any J2EE compliant Application Server such as Tomcat, Websphere and Weblogic. We recommend that you use Tomcat Version 6.x.

Lotus Notes Setup

Overview

When connecting to Lotus Notes, the integration uses an additional piece of software called the Domino Bridge. A small web application is deployed either on the Domino Server or a separate web server that accepts secure SOAP requests and translates these into calendar events. The web application uses a minimal-access delegate account to connect over DIIOP to your Domino server and create calendar entries on behalf of users.

Note: Enterprise Groupware for Lotus Notes is a Premium Service and requires a separate agreement with Deem to be in place before configuration can take place. If you are unsure if your agency has this service included in your reseller agreement with Deem, enter a support case (see Entering a Support Case for instructions).

You need the following:

- A J2EE compliant Application Server for the Integration Service to run in. Any J2EE compliant Application Server such as Tomcat, IBM Websphere, JBoss and BEA Weblogic will work. We strongly recommend Tomcat Version 6.x as the integration has been thoroughly tested with Tomcat 6.x. It can be downloaded from http://tomcat.apache.org/download-60.cgi. You will need the binaries only.

  Note: Do not use the native Domino Server due to potential conflicts with the IBM JDK version that Domino needs versus the Sun Microsystems, Inc. JDK 6.0 version that the groupware integration requires

- Java JDK 6.0, which can be downloaded from http://www.oracle.com/technetwork/java/javase/downloads/jdk6u38-downloads-1877406.html. Select the version without the NetBeans IDE. You do not need to install the Java Runtime Environment (JRE) separately either.

  Note: We strictly require JDK 6.0 due to dependencies with certain libraries. If you have any other version, we recommend that you have a separate JDK 6.0 instance running for the groupware integration.

Preparing Your Environment

Consult your Domino/System administrator when deciding on where to deploy the web application. You have two options

- Deploy the web application on the same physical device as the Domino Server.
- Deploy the web application on a separate physical device.

Note: If you have an environment that has multiple Domino Servers, you need to pick one of those as your “master” Domino Server and have that server communicate with the web application.

You will need to make sure that the device has the correct JDK and Tomcat version installed. Follow the steps below to ensure that your device is ready for the web application (WAR) deployment:

1. Ensure that the JDK environment is correctly set up. (You may skip this step if you already have JDK 6.0 on the device that you plan to install the web application.)
   Click here to expand...
   a. Install JDK 6.0 from http://www.oracle.com/technetwork/java/javase/downloads/jdk6u38-downloads-1877406.html.
   b. Once you have run the installer, make sure that the environment variables are set correctly:
      - For Windows, add the path to the ‘bin’ directory of your JDK installation to the “PATH” environment variable. Choose **My Computer>Properties> Advanced>Environment Variables**. Edit the “PATH” variable and add the path to the ‘bin’ directory. For example:
        PATH = C:\Program Files\Java\<JDK version>\bin
      - For UNIX, export PATH="${JAVA_HOME}/bin:${PATH}”
2. Install Tomcat 6.x. (You may skip this step if you already have Tomcat 6.x on the device that you plan to install the web application.)
   Click here to expand...
   a. Install Tomcat from http://tomcat.apache.org/download-60.cgi . You will need the core binaries. You may choose to install the “Windows Service Installer” version.
   b. Make sure that the JAVA_HOME environment variable points to the JDK home directory:
      - For Windows, JAVA_HOME = <Path to the JDK directory>, e.g. C:\Program Files\Java\<JDK version>

- For Unix, export JAVA_HOME="/usr/java/<JDK version>

c. Once you are done with the Tomcat installation, the best way to confirm if it installed correctly is to type the following in your browser (http://localhost:8080/ OR http://<machine name/IP address>:8080/). If you see the tomcat page, then the installation went through successfully.

3. Prepare the Domino Server For integration.
   Click here to expand...
   a. Create a Delegate User on the Domino Server. You would create the delegate user like any other on the Domino Server; we recommend that you call it the “Deem Delegate” or simply “Delegate”. Since the integration users the delegate credentials to access user calendars, it is a good practice to make sure that the password for the user never expires. This will ensure that the integration works uninterrupted.
      Note: If you do not have a password that never expires, the web application will need to be redeployed every time the password is changed.
   b. Enable DIIOP on the Domino Server. You do this by executing the command **load diiop** at the Domino command prompt (>).
   c. Configure Domino to start DIIOP whenever the servers are restarted. You do this by editing the notes.ini file and adding “diiop” to the end of the “ServerTasks = “ line.

Deploying the Integration Web Service

Before you start the web application deployment, make sure your environment is ready. You should have the following information with you before you deploy the web application:

- Domino Server machine name
- Domino server DIIOP port number (Default value is 63148)
- Delegate user id and Delegate Internet password
- Decide on a service password. You will need this when you generate the WAR file, and it has to be the same value when you configure the groupware server.

Download the TAR file.

We recommend that you download it to the same device that will have Tomcat installed. We also recommend that you download it in a separate folder called “DeemIntegrations”. This makes it easy to go locate the files needed and also serves as an archival mechanism for the WAR files generated. Once you have downloaded the TAR file to the \DeemIntegrations folder, follow these steps:
Click here to expand...

1. Unzip the TAR file and keep the directory structure intact.
   a. On Unix : tar xvf groupware.tar
   b. On Windows : unzip using Winzip or equivalent
2. The unzipped/untared file will generate a groupware directory. On Unix, give executable permissions (for example, "chmod +x groupwareWebservicesSetup.sh"). Change the active directory to the groupware directory created in Step 2.
3. By default a log file called RCGroupware.log will be created in the directory from where the web server is started, to change the location of log file, edit the file "groupware\WEB-INF\classes\log4j.properties" and set the property "log4j.appender.groupwarelogfile.File" to the absolute path of the log file.
4. Run the groupware web service setup utility. Make sure you have the Domino Server machine name, Domino server DIIOP port number, Delegate user ID and delegate password handy.
   a. On Unix: Run the script groupwareWebservicesSetup.sh
   b. On Windows: Run the script groupwareWebservicesSetup.bat
      Note: If need to get that TrustedCerts.class file into the classes directory once you've deployed to the web app container.
5. The script will prompt you to enter the following information:
   a. Domino Server Address : <Enter domino server machine name /IP Address>
   b. Domino Server Port : <Enter the DIIOP port number , default is 63148>.
      Note: Domino server should have DIIOP server running; contact your Domino admin if DIIOP is not enabled on the server.
   c. Delegate User Id : <Enter the User Id of the delegate >
   d. Delegate User Internet Password : <Enter the delegate password>
      Note: Web services uses this delegate's credentials to login to the Domino Server to perform the calendar operation. Make sure the delegate account is created before deploying. Also make sure that the delegate is assigned an Internet password and that the password is the one utilized in the WAR file.
   e. Enter Service Password : <Enter the service password>
      Note: this is the same password that is entered as service password while configuring the groupware server. The password is encrypted for security.
6. Once the above configuration is entered, a groupware.war file is generated in same directory, deploy this war on the web server. For Tomcat, you simply need to copy this WAR file in the \webapps directory and restart the Tomcat Server.

To test whether the deployment was successful, restart the Tomcat Server and go to the following URL:

http://localhost:8080/groupware/services/groupware

or

http://<Macine name/IP address>:8080/groupware/services/groupware

In order to configure a Customer Groupware Server Configuration, we need the following information:

- Web Services endpoint URL (e.g., http://10.5.3.239:8080/groupware/services/groupware)
- Three or Four email addresses
    - Randomly selected from users to whom permissions for the delegate account have been applied
    - Used in testing application of the permissions
- Send to integration@deem.com and to your Activation Manager or Deployment Manager.
- Send Service Password only to integration@deem.com, or send a request to contact you and get the password over the phone.

Applying Delegate Permissions Using the Delegate Utility

Before running the following script, make sure that all the user ids or email ids for whom the delegate needs to be set are listed in a file called <users>. Each id should be listed in a new line. For the utility to work, all the users listed in the users file should have the "maximum internet name and password" setting set to Manager Level. In the Domino Administrator Console, this setting is in the user's ACL manage screen under Advanced tab. Alternatively the same setting can be set on the mail folder to take effect on all the users' mail files in the folder.

Note: The "maximum internet name and password" only needs to be set to "Manager" level while the delegate permissions are being applied by the delegate utility. Once permissions are set, this setting can be reverted back to its original level.

1. Run the Delegate Utility located provided in the downloaded TAR files.
    a. On Unix/Linux run the script delegateSetupUtil.sh
    b. On Windows run the script delegateSetupUtil.bat
2. The script will prompt you to enter the following information:
    a. Domino Server Address : <Enter the Domino server machine name /IP Address>
    b. Domino DIIOP Port : <Enter the DIIOP port number , default is 63148> (Note : Domino server should have DIIOP server running , contact domino admin if DIIOP is not enabled on the server)
    c. Delegate Id : <Enter the User Id of the delegate >
    d. Delegate Domain: <Enter the delegate users domain >
    e. Administrator Id : <Enter the Domino Administrators user id>
    f. Administrator Password : <Enter the Domino Administrators Password>

The utility creates an ACL entry with the following permission for the entered delegateID/delegateDomain for all the line delimited users listed in <users> file:

- User Type: Person
- Access: No Access
- Read Public documents - true
- Write public documents <96> true
- Rest all are set to false.

If the user already has the ACL set for the delegateID/delegateDomain set, then it will update the ACL with above permission set.

Applying Delegate Permissions Using Domino Administrator

Rather than using the delegate utility provided, the delegate permissions can be applied using Domino Administrator by following these steps:

- Once in Domino Administrator, drill down to the mail file (Or mail folder if applying to all users) you wish to set permissions for.
- Choose **ACL>Manage** to access ACL for user (Or folder).
- Click **Add…** to add the delegate account to the user's (Or folder's) ACL.
- Once delegate account is added, under Attributes select **No Access**.
- Click **Read public documents** and **Write public documents**.

Enabling the Groupware Server in the Partner Dashboard

The Deem Activations team or your system administrator enables enterprise groupware in the Partner Dashboard by following these steps:

1. Log into the Partner Dashboard as the site administrator.
2. Click the **Groupware Servers** link under the Settings tab.
3. Click the **Add Server** link to show the Add Server page and add a server, or click the link for an existing groupware server to show the Edit Server page and edit the server's settings.
4. If adding a server, enter a Server or Gateway name for easy identification when choosing servers for groups.
5. Choose the server type from the Server Type drop-down menu: **Lotus Notes Integration Service**.
6. Click the **Save** button to save the server settings.

7. To commit these changes, click the green **Changes not applied** link in the top right corner of the page, and then click the **Commit** button .

Assigning the Groupware Rule to a Group

To assign the groupware rule to the group, follow these steps:

1. Log into the Partner Dashboard as the site administrator.
2. Click the **Rules** tab, and then click the **Groupware Rules** link.
3. Click the **Add** button next to the group name (or the Everyone group).
4. Enter a Rule Description that describes the intent of this rule, and click the Activate Rule checkbox.
5. Scroll down to the “Then” section of the page, and click the “Enable groupware access” checkbox.
6. Select the server or gateway name (the name you entered in Step 4 in the previous steps for adding the groupware server) from the Use Groupware Server drop-down menu, and click the “Enable calendar updates on this server” and “Enable address book lookups on this server” checkboxes.
7. Click the **Save** button to save the settings.
8. To commit these changes, click the **Changes not applied** link in the top right corner of the page, and then click the **Commit** button.

Web Services SOAP API

The Web Services for add, delete, and modify events are illustrated in the **Web Services SOAP API**.