IBM Atlas Suite Administrators Guide: System Configuration

for IBM Atlas Suite v6

IBM

IBM Atlas Suite Administrators Guide: System Configuration

This edition applies to version 6.0 of IBM Atlas Suite (product numbers 5725-D75, 5725-D76, 5725-D77) and to all subsequent releases and modifications until otherwise indicated in new editions.

Contents

1 Introduction

This book guides a System Administrator through the configuration of IBM Atlas Suite. The configuration instructions are given in roughly the order that you would follow them to configure a freshly deployed system. A number of the chapters in this book refer to other IBM Atlas Suite Administrators Guides for detailed instructions and descriptions. To complete the instructions in this book, and for more advanced configuration topics, you'll also need these books:

- **IBM Atlas Suite Administrators Guide: Components**
- **IBM Atlas Suite Administrators Guide: Timer Tasks**
- **IBM Atlas Suite Administrators Guide: Events**
- **IBM Atlas Suite Administrators Guide: Drop Boxes**
- **IBM Atlas Suite Administrators Guide: Atlas Extensions**
- **IBM Atlas Suite Administrators Guide: Importing Data through CSV Files**

1.1 System Configuration for Upgraded Systems

If you're upgrading your IBM Atlas Suite system (as opposed to a installing a fresh deployment), you'll have already performed most of the configurations that are described in this book. While you should still step through all the chapters, you should pay particular attention to the following:

- Creating Matter Metrics (Upgrade Only). The *Matter Metrics* feature was added to IBM Atlas Suite v6. The feature provides statistics about the Legal Matters that are in the system. In order to create continuity with pre-v6 Matter activity, you must run a script that analyzes and incorporates this existing data.
- Notice Templates and User Password Messages. In IBM Atlas Suite v6, Notice Templates (the **Admin > Notice Templates** module) are no longer used to create the body of a Hold Notice. If you have a library of Notice Templates that you want to continue using as the bases for Hold Notice bodies, you have to recreate these Templates in the new **Admin > Hold Notice Templates** module.
- Hold Notice Templates. The construction of Legal Hold Notices changed significantly in v6. Paralegals can no longer create a Notice from scratch; instead, they must create Notices by selecting a pair of *Hold Notice Templates*. As there are no default Hold Notice Templates, a System Administrator must create the Templates, through the **Admin > Hold Notice Templates**, before new Hold Notices can be authored.

NOTE The Hold Notices that were created and published before upgrading to v6 will continue to work as expected. However, a Notice author can transform old Notices into v6 versions in order to take advantage of the new Hold Notice features. Instructions for transforming old Notices are given **in IBM Atlas Suite User Guides: Hold Notices**.

- Global Hold Reminder. IBM Atlas Suite v6 introduced the *Global Hold Reminder*. This is a "bulk" Auto-Reminder for Hold Notices: Instead of sending individual Auto-Reminders for each of the Holds that a Custodian is part of, the system can send a single Global Hold Reminder that asks Custodians to go to the **My Holds** module and review their obligations. To use this feature, you must configure and activate the Global Hold Reminder through the **Admin > Global Hold Reminder** module.

- Matter Exceptions and Alerts. IBM Atlas Suite v6 introduced *Matter Exceptions*. These are time-based measures that detect if a Matter is stalled. For example, if a Notice spends too much time waiting for approval, the Matter's "exception score" is heightened. Legal users can sort the Matters list (in the **Matters** module) based on these scores, thus allowing them to identify the Matters that need immediate attention.

  Similarly, system Alerts (all of them—not just those that pertain to Matters) can be marked as **Warning**, **Important**, or **Critical**. These rankings are used to filter the Alerts that are displayed in a user's **My Alerts** tray on the **My Atlas** page.

2 Preparation, Tips, and Caveats

This chapter tells you how to prepare your system for configuration, and provides some suggestions for improving performance and functionality.

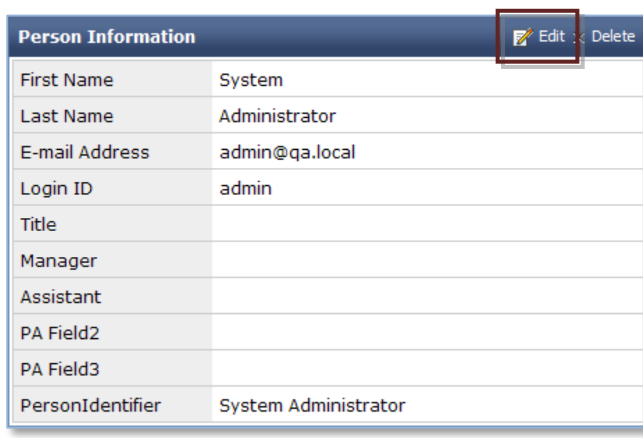
2.1 Synchronize your Servers

It’s essential that you synchronize the system time on your database and application servers. If the servers fall out of sync, some requests might not take effect until the next day.

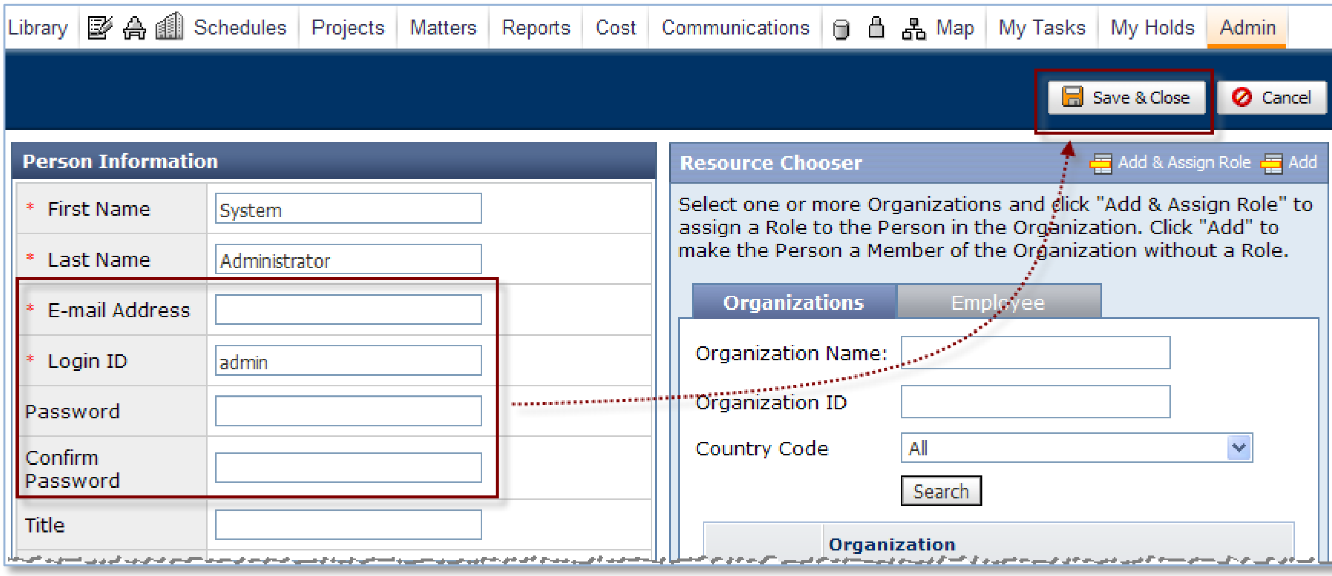
2.2 Reset the System Administrator Account

When you deployed IBM Atlas Suite, a System Administrator account with a default username and password (**admin/admin**) was created for you. You should log into the Atlas application and change the System Administrator account information.

1 Go to the **Admin > Persons** module, select the “**Administrator, System**” account, and click **Edit**.



2 The information panel will become editable. Reset the account's email address, login ID (if you want), and password, and then click **Save & Close**:



Atlas sends system health messages to the System Administrator account; choose an email address appropriately.

2.3 Person Identifier Resolution

The system lets you declare whether or not the **Person Identifier** for Person records is required and must be unique. The declaration is made by setting the value of the **PA_DATA_INTEGRITY > UNQ_PERSONIDENTIFIER** Component Parameter: If it's set to **Yes**, the Person Identifier is required and must be unique; if it's **No**, (the default) the Person Identifier is optional and needn't be unique. You must set the value of the Parameter before you ingest Person data.

2.4 Purging the PolicyAtlasAudit Table

When certain business objects are created, modified, or deleted, the system adds a record to the **PolicyAtlasAudit** table in the database. Later, when the *Change Alert Timer Task* runs, each new record triggers a *Change Alert* that notifies users of the change. The **PolicyAtlasAudit** table is never purged of data and thus can grow to be quite large. As the size of the table increases, the amount of time it takes to generate and send the Change Alerts also increases. If the table becomes too big, system performance can become degraded

If you're concerned with Change Alert performance, you may want to purge the **PolicyAtlasAudit** table yourself, either by hand or through a script. To properly purge the table, you need to understand the following:

- The **PolicyAtlasAudit** table doesn't just contain records that trigger Change Alerts. To identify the Change Alert triggers, look at the value of the **PAField4** column. For Change Alert triggers, the column's value is **ALERT_PULL_RECORD**.
- You only want to delete Change Alert triggers that have already been processed by the Change Alert Timer Task. After the Task is finished with a Change Alert trigger, it sets the record's **ChangeAlertStatus** value to **Done**. If a Change Alert trigger doesn't have a status of **Done** it shouldn't be deleted.

- When a Change Alert trigger is created, its **ModifiedOn** value is set to the current day and time. You might want to only delete records that are of a certain age; 60 days is recommended.
- You may want to consider archiving the Change Alert records that you're about to delete.

How you archive and purge the **PolicyAtlasAudit** table is up to you.

2.5 Improving Database Performance

You can improve the performance of the database by telling Oracle to measure the amount of data it contains. To do this, launch SQL*Plus as the **PSSAPL** user and execute the procedure that gathers statistics:

```
$ sqlplus PSSAPL/PSSAPLPWD@DBName
SQL> EXEC dbms_stats.gather_schema_stats('DBName', cascade=>TRUE,
estimate_percent=> DBMS_STATS.AUTO_SAMPLE_SIZE);
```

The command will take a few minutes to complete.

To maintain peak performance, you should run this procedure periodically.

IMPORTANT	You can run the statistics gathering procedure at any time, but, you should *definitely* run it after the first time you ingest your company's business data.

2.6 Browser Arrow Navigation

You should advise your Atlas users that they shouldn't use their web browser's back and forward arrows to navigate pages in Atlas. Instead, they should use the breadcrumb links that are displayed near the top of most modules, or use the other module-specific navigation controls that Atlas provides.

For example, if a user creates a Hold Notice that will use a Virtual Interview for confirmation and then visits the VI creation page (by clicking **Create VI**) to define the VI plan, the user must click the **Hold Notice** button (on the VI page) or the Hold Notice's name in the breadcrumb to get back to the original Hold Notice. Clicking the web browser's back arrow won't work.

2.7 Web Browser Session Caveat

Both Internet Explorer and Firefox automatically share the existing browser session when a new window or tab is opened. However, IBM Atlas Suite doesn't support the use of shared browser sessions. If a user logs into Atlas more than once at the same time on the same machine (through separate windows or tabs), the data that the user specifies in one window/tab will overwrite the data that's specified in the other window/tab.

Because of this constraint, you should advise your Atlas users that they mustn't log into Atlas more than once at the same time on the same machine. Alternatively, users can work around this constraint if they're using Internet Explorer (there's no easy workaround for Firefox):

- In Internet Explorer 7, users must launch a new instance of IE for each concurrent Atlas login session. They should *not* use **Ctrl+N** or **Ctrl+T** to create a new window or tab.
- In Internet Explorer 8 and 9, users must specifically ask for a new session through the **File > New Session** menu item. Launching a new instance of the browser is *not* sufficient. As with IE 7, users must also not use **Ctrl+N** or **Ctrl+T**.

2.8 ActiveX Control

After an upgrade, the ActiveX Control that's installed on Atlas users' machines so they can upload collected files might become obsolete. In this case, the user is prompted to download and install a new version.

If your company doesn't allow users to download and install applications themselves, you'll need to install the new ActiveX Control for them, as described in the **ActiveX Control** section of the *Low-level Configuration* chapter.

3 Creating Matter Metrics (Upgrade Only)

NOTE This chapter only applies to systems that are being upgraded from a pre-v6 release to IBM Atlas Suite v6 or later.

The *Matter Metrics* feature was added to IBM Atlas Suite v6. The feature provides statistics about the Legal Matters that are in your system. The statistics for the day-just-ended are generated every night by a Timer Task (if you're using the recommended settings).

If you're upgrading from a pre-v6 release to IBM Atlas Suite v6 (or later), you need to run a script that will analyze your existing (pre-v6) Matter data. However, depending on the number and complexity of the Matters in your system, the analysis could take a long time—as much as several days—and could consume significant amounts of database processing and resources. Because of this, you can stop the script at any time, and restart it later without losing the analysis from previous runs—you may want to run it only at night or on the weekend, for example.

Furthermore, while the analysis script should be run as soon after deployment as possible, it must not be run until *after* the daily Timer Task (**Matter Metrics Extraction**) has run at least once.

To run the script, do this:

1. Log into the Atlas application go to **Admin > Timer Tasks**, and click the name of the **Matter Metrics Extraction Task**.
2. You'll be taken to a page that lists the Task's executions. Make sure that the Task has completed successfully (the **Status Code** should be **SUCCESS**).
3. On the database client machine, open a shell and execute the following script:

```
$ cd
C:/ATLAS/Schema/Deploy/smf/db/release/default/oracle/create/data/historical_metric
$ sqlplus -s PSSAPL/PSSAPLPWD@DBNAME @populate_historical_metric
```

4. If you need to kill the script as it's running, type `Ctrl-c`. As mentioned above, you can restart the script later and it will pick up where it left off.

As it's running, the script displays its progress. Note that the script analyses historical data in reverse chronological order:

```
Populating historical metrics from 02-AUG-07 to 24-AUG-10
  Note: The process may take several hours...
  Metrics for 24-AUG-10 1 sec.
  Metrics for 23-AUG-10 1 sec.
  Metrics for 22-AUG-10 2 sec.
  etc…   .
```

When the script has finished, it prints the following message and returns you to the command line:

```
Populating historical metrics done
$
```

You only need to run the script to completion once.

4 Low-level Configuration

This chapter tells you how to configure low-level features that apply to all of IBM Atlas Suite, and that must or should be configured before the application can be used by non-administrators.

To use this chapter, you need knowledge of and access to your company's IT infrastructure (file systems, email servers, and so on) and you should understand which of the IBM Atlas Suite products and features your company is using. You need very little business knowledge to perform the configurations that are listed here.

4.1 Email Settings

4.1.1 Email Servers

The **MAILSETTINGS** Component identifies your system's SMTP and POP servers. During initial configuration, you should configure these Parameters:

- **SMTPSERVER**
- **SMTP_PORT**
- **SMTP_REQUIRES_AUTHENTICATION**
- **SMTP_USERNAME**
- **SMTP_PASSWORD MAX_RECIPIENTS_COUNT**
- **RETRYCOUNT**
- **APPSERVERURL**
- **POPSERVER**
- **POP_PORT**

You can also configure the Component's other Parameters (**FromAddress**, **NoticeFrom**, and so on), although they may require more business knowledge than is available during initial configuration. The Component is described in the *Low-level Configuration* chapter of the **IBM Atlas Suite Administrators Guide: Components** book

MAIL_DNS_LOOKUP. This Component sets the type of DNS resource record that's used by Atlas when it resolves the domain names of outbound email messages. The default is type **A**; if you need to use a different type (for MTA load-balancing, for example), you must configure this Component.

4.1.2 Confirmation Mailboxes

The **EMAIL CONFIRMATION MAIL SETTINGS** Component manages the reply messages that are created and sent back to the system when a user responds to a Hold Notice. Configuring the Component could require more business knowledge than is available during initial configuration; however, you should consider creating three email accounts as explained in the descriptions of these Parameters:

- **EMAIL CONFIRMATION MAILBOX**

- **EMAIL CONFIRMATION MAILBOX USERNAME**
- **EMAIL CONFIRMATION MAILBOX PASSWORD**
- **PROCESSED_MAILBOX**
- **ERROR_MAILBOX**

You should also configure these two Parameters to match the constraints of your mail servers:

- **END_OF_LINE**
- **USER_TRACKER_ID**

4.2 Log Files

In this section you'll identify the locations of the log files that are generated by Atlas.

4.2.1 Atlas and Application Server

The **PA_CONFIGURATION** Component contains Parameters (**APP_SERVER_LOG_FILE_PATH** and **POLICY_ATLAS_LOG_FILE_PATH**) that tell the system where to find the log files for the application server and for the Atlas application, respectively. These values are used as the targets of the **View App Server Log** and **View Atlas Log** links on the **Admin** page. The log files aren't meant to be customer-readable; if you have a technical problem your IBM ECM Client Technical Professional may ask you to send the log files.

4.2.2 CSV Import

The **CSV_IMPORT** Component tells Atlas where to create (not just find) the log file that reports on the success of the CSV import attempts. The CSV log file *is* meant to be customer-readable. You should review the log file each time you import a CSV file.

4.3 System Health

This section describes the functionality that helps you judge the health and status of the Atlas applications.

4.3.1 System Monitoring

IBM Atlas Suite can be integrated with application monitoring programs such as Tivoli, BMC Patrol, or other common IT tool. The **IBM Atlas Suite Administrators Guide: Monitoring the System** lists the system elements that can be monitored and describes the error and status messages that they produce.

4.3.2 The Oracle Monitor Job

The Oracle database schema includes an optional *Monitor Job* that sends an email to a recipient of your choice if the Legal Notice or Alert system isn't working properly. The IBM Atlas Suite Deployment Guide describes how to configure the Monitor Job during initial deployment. The instructions for configuring the Monitor Job *after* you've deployed are given here. To follow the instructions, you must have SYSDBA privileges.

IMPORTANT	To use the Monitor Job, your database server must be able to access your SMTP server.

To complete the instructions you'll need this information:

- The TNS name of the database instance or net service (**`TNSName`**).
- The name and password of a SYSDBA account (**`SYSTEM`**/**`SYSTEMPWD`**).
- The name and password of the IBM Atlas Suite schema owner (**`PSSAPL`**/**`PSSAPLPWD`**).
- The location of the Atlas installation directory (**`C:/ATLAS`**)
- The host name and port number of your SMTP server (**`MailHost`**, **`MailPort`**).
- The email address of the person who should receive the email.
- The email address that's used as the **From:** address in the email.

Follow these steps:

1 Log into the database client machine that Atlas is installed on and open this file in a text editor:

`C:/ATLAS/Schema/Deploy/smf/db/release/default/oracle/create/source/plsql/pkg/monitor_pack.sql`

2 Look for this block of parameters:

```
c_mail_host CONSTANT VARCHAR2(64) := '&p_MailHost';
c_mail_from CONSTANT VARCHAR2(64) := '&p_MailFrom';
c_mail_to   CONSTANT VARCHAR2(64) := '&p_MailTo';
c_smpt_port CONSTANT NUMBER       :=  &p_SmtpPort;
```

Remove the placeholders and supply parameter values that are valid for your system (*don't* remove the single quotes):

- Replace **`&p_MailHost`** and **`&p_SmtpPort`** with the host name and port number of your SMTP server.
- Replace **`&p_MailTo`** with the email address of the person who should receive the email.
- Replace **`&p_MailFrom`** with the email address that's used as the **From:** address in the email.

3 Save and close the file.

4 Compile the file as the **`PSSAPL`** user:

```
$ cd C:/ATLAS/Schema/Deploy/smf/db/release/default/oracle/create/source/plsql/pkg
$ sqlplus PSSAPL/PSSAPLPWD@TNSName @monitor_pack.sql
```

5 `cd` to the directory shown below and execute the `grant_acl_sendmail.sql` script as the `SYSTEM` user. This will give the Monitor Job sufficient privileges to send email:

```
$ cd C:/ATLAS/Schema/Deploy/smf/db/release/default/oracle/create/user/
$ sqlplus SYSTEM/SYSTEMPWD@TNSName @grant_acl_sendmail.sql PSSAPL MailHost MailPort
```

4.3.3 Timer Task Framework

A number of system functions—such as generating Alerts and sending email messages—are performed through *Timer Tasks*. These are background jobs that wake up according to a schedule, perform their tasks, and then go back to sleep. The Timer Task framework and the Tasks themselves are described in detail in the **IBM Atlas Suite Administrators Guide: Timer Tasks** book.

During initial configuration, you should at least review the default values of Parameters in the **TIMER-CONFIGURATION** Component. These Parameters establish the process that oversees the Timer Task framework. If the process senses that the Timer Tasks aren't operating properly, it sends an alert to the system administrator.

You can also use the **Admin > Timer Task Configuration** module to enable/disable individual Timer Tasks and set their frequencies, although that may take more business knowledge than is available at this point. The Timer Tasks that apply to specific modules will be described in later chapters of this book.

4.4 Licensed Features

The following Components and Parameters enable and disable the licensed features of Atlas.

Feature	Component > Parameter
IBM Retention Policy and Schedule Management	**ERM_INSTALLED > ERM_INSTALLED**
IBM Atlas eDiscovery Portal for Employees	**PA_CONFIGURATION > ENABLE_EMPLOYEE_PORTAL**
IBM Atlas IT eDiscovery Process Management	**PA_CONFIGURATION > ENABLE_IT_PORTAL**
IBM Disposal and Governance Management for IT	**PA_CONFIGURATION > ENABLE_POLICY_DISTRIBUTION** **DS_CONFIGURATION > IIM_ENABLED** **DS_CONFIGURATION > ENABLE_ERM_DS_BY_APPROVER**

4.5 Application and Subsystem Integration

In this section, you'll tell IBM Atlas Suite how to communicate with and transfer data between other applications and subsystems.

4.5.1 Atlas Reports

Atlas Reports is a separate application that generates report files for the Atlas application. To configure Atlas Reports, see the Atlas Reports Configuration chapter.

4.5.2 Employee Retention Portal

The Employee Retention Portal is an application that lets Atlas users view the retention policies that apply to them. To install and configure the Employee Retention Portal, see the **IBM Atlas Suite Administrators Guide: Employee Retention Portal** book.

4.5.3 Document Library

When a user uploads documents into the system, the document files are placed in a temporary directory on the application server where they wait to be processed (copied into the database, parsed by the CSV importer, and so on). After they've been processed, they're removed from the temporary directory. Similarly for documents that are downloaded (or exported) from the system: The files are copied into the temporary directory where they wait to be downloaded to the user's machine.

The **DOCUMENT_LIBRARY** Component configures the document import and export feature. Most importantly, the **TEMP_DIRECTORY** Parameter sets the location of the temporary directory. You must set the value of this Parameter to a directory that already exists; the system won't create it for you. On UNIX systems, the directory must have read/write/execute permissions for the owner.

In addition to setting the **TEMP_DIRECTORY** Parameter, you should review the values of the Parameters that set size limits and timeouts on the data that's moved between the system and the temporary directory, and you should also make sure that the **ESCAPE CHARACTERS DURING EXPORT** matches the characteristics of the file system in which the temporary directory resides.

4.5.4 External Repository

The External Repository feature lets you store imported files in your own file system rather than in the Atlas database. This section tells you how to enable the External Repository *after* you've deployed the database. To complete the instructions you'll need this information:

- The name of the database instance or net service (**`TNSName`**).
- The name and password of a SYSDBA account (**`SYSTEM`**/**`SYSTEMPWD`**).
- The name and password of the IBM Atlas Suite schema owner (**`PSSAPL`**/**`PSSAPLPWD`**).
- The location of the IBM Atlas Suite installation directory (**`C:/ATLAS`**)

To enable the External Repository, follow these steps:

1 Log into the Oracle client machine and open this file in a text editor:

`C:/ATLAS/Schema/Deploy/smf/db/etc/oracle/smf_properties.ini`

2 Set the `DATABASE_JAVA_PRIV` and `ER_ENABLED` flags to `Y`. Save and close the file when you're finished:

```
DATABASE_JAVA_PRIV      = Y
ER_ENABLED              = Y
```

3 Grant Java privileges to the Atlas schema owner:

```
$ cd C:/ATLAS/Schema/Deploy/smf/db/release/default/oracle/create/user/
$ sqlplus SYSTEM/SYSTEMPWD@TNSName @grant_java_priv.sql PSSAPL
```

4 Load the External Repository settings:

```
$ cd C:/ATLAS/Schema/Deploy/smf/db/etc/python/
$ java.exe -jar ../../lib/jython.jar loadERJar.py -u PSSAPL-p PSSAPLPWD
```

IMPORTANT	If you're using an External Repository, you must make sure that the application server is configured to connect Atlas to the database through the `PSSAPL` account (*not* `PSSWEBUSER`).

After you've enabled the External Repository, you must tell Atlas where your repository is by setting the **ROOT_LOCATION** Parameter in the **EXTERNAL_REPOSITORY** Component.

4.5.5 ActiveX Control

IBM Atlas eDiscovery Process Management provides an ActiveX control that makes it easy for users to upload documents that they've collected for a legal matter. By default, the control is automatically downloaded to a custodian's desktop the first time the custodian responds to a collection notice. In some companies, however, security protocols prevent application downloads, and so the ActiveX control must be pre-installed on the employees' machines.

The ActiveX control is in the IBM Atlas Suite distribution:

`ATLAS/AddOns/ActiveXControl/IBMAtlasSuiteUpload.ocx`

The control can be installed directly on users' machines.

4.5.6 PST Extractor

PST Extractor is an application that lets IBM Atlas Suite users search the contents of the Outlook archive files, email messages, and attachments that have been uploaded to Atlas. The application extracts messages from Outlook email archives (PST files) and attachments from individual messages (MSG files), and then sends the extracted data back to Atlas for indexing.

PST Extractor installation and configuration is described in the **IBM Atlas Suite Administrators Guide: PST Extractor** book.

4.6 Data and Filename Management

The Components listed below manage data cleanup or manipulate filenames to fit the characteristics of your platform.

4.6.1 Data Purge

The **DATA_PURGE_SETTINGS** Component sets the time period after which the database is purged of old, unneeded data. During initial configuration, you should review the default settings of these two parameters:

- **APPLICATION_EVENT_LOG**
- **SYSTEMPROCESSLOG**

You should ignore the other three Parameters (***_STAGING**). These are used by the Atlas Extensions application; setting these Parameters requires coordination with other Atlas Extensions configuration variables and is described in the **IBM Atlas Suite Administrators Guide: Atlas Extensions** book.

The data purge is performed by the **TempTableCleanup Task**. By default, the Task runs once a day at 11:30 pm. If you want to change the execution time, see the **Atlas Administrators Guide: Timer Tasks** book for guidance.

4.6.2 File System Constraints

The **TRUNCATE_FILENAME_DURING_EXPORT** Component provides rules for modifying the names of files that are exported from the system. This can help you avoid overly-long pathnames and illegal characters that are generated when a set of collected files is exported. For a complete explanation of this Component, including examples, see the **Exporting Documents from Legal Matters** book.

4.6.3 Individual Collection Tool

The **PA_CONFIGURATION > INDIVIDUALCOLLECTIONTOOL** Parameter determines the type of control that's presented to users who upload documents into the system. If you set it to **ActiveX**, users are presented with a drag-and-drop ActiveX control. However, you must make sure that the control, which is part of the IBM Atlas Suite distribution, can either be downloaded to the user's computers on demand, or that it has been pre-installed on those computers, as explained in ActiveX Control.

If you're not using the ActiveX control, remove the **INDIVIDUALCOLLECTIONTOOL** value. By doing so, users will find and upload files through a normal Windows file browser control.

4.6.4 License Report

If the Automatic License Report feature is enabled, IBM Atlas Suite will generate a license report some number of times a year and send it to a designated email account. Your IBM ECM Client Technical Professional will help you determine if the report needs to be generated more or less often, and where it should be sent. This information (including a Parameter that enables and disables the feature) is configured in the **AUTOMATIC_LICENSE_GENERATION** Component.

5 Interaction with Windows Internet Information Server (IIS)

If you're using the Windows Internet Information Services (IIS) 6.0 or 7.0, you can let IIS act as a proxy that mediates communication to and from the Atlas applications, and that can act as the point of entry for Single Sign-On authentication.

It's recommended that you use Helicon Tech ISAPI Rewrite 3 as the interface between Atlas and IIS. The Helicon Tech software reads the encrypted user ID that's delivered in the IIS authentication request, decodes it, and then passes the decoded ID to Atlas.

IMPORTANT	You must obtain the licensed (paid) version of ISAPI Rewrite 3. The free version doesn't contain the proxy functions.

This chapter tells you how to configure IIS, how to install and configure Helicon Tech ISAPI Rewrite 3, points you to instructions where you'll configure SSO (if you're using SSO), and then shows you how to test the connection.

IMPORTANT	The configurations described in this chapter are required if your Windows Security Policy enforces NTLMv2 *only*. If it uses LM or NTLMv1, you should skip this chapter.

5.1 Configure IIS

To configure IIS, you must enable authentication and then tell IIS about IBM Atlas Suite. How you enable authentication depends on the version of IIS that you're using:

- The instructions for IIS 6.0 are here:

  http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/5f8fe119-4095-4094-bba5-7dec361c7afe.mspx?mfr=true

- The instructions for IIS 7.0 are here:

  http://technet.microsoft.com/en-us/library/cc754628(WS.10).aspx

To tell IIS about IBM Atlas Suite, perform the following instructions on your Windows IIS machine:

1. In the file system, create a **`C:/ATLAS`** directory.
2. Launch **IIS Manager**.
3. Right click the **Default Website** and select **New > Virtual Directory**. This will open the **Virtual Directory Wizard**.
4. In the first screen, set **Alias** to **PolicyAtlas** and click **Next**.
5. In the next screen, set the **Folder** to **`C:\ATLAS`** and click **Next**.

6 In the **Permissions** screen check the following checkboxes:

- **Read**
- **Run Scripts**
- **Execute**

7 Click **Next** and then **Finish**.

8 Back in the main window, right-click the new **Atlas** web site icon and select **Properties**.

9 In the **PolicyAtlas Properties** panel, click the **Directory Security** tab.

10 In the **Authentication and access control** section, click **Edit…**.

11 In the **Authentication Methods** panel:

- Uncheck the **Enable anonymous access** checkbox.
- Check the **Integrated Windows authentication** checkbox.

12 Click **OK** to dismiss the panel.

13 Exit **IIS Manager**.

5.2 Install and Configure the Helicon Tech Software

After IIS has authenticated an IBM Atlas Suite user, it sends the user's credentials to an Internet Server Application Programming Interface (ISAPI) which filters the credentials and then passes them on to the Atlas application. It's recommended that you use Helicon Tech ISAPI Rewrite 3 as the interface between IBM Atlas Suite and IIS. You can purchase and download the Helicon Tech software by going here:

http://www.helicontech.com/order/#isapi_rewrite3

Download the software and install it on your Windows IIS machine. Accept the defaults that the installer presents.

NOTE As it's running, the ISAPI installer may restart the World Wide Web Publishing Service. This is normal.

To configure Rewrite 3, do this:

1 Open the configuration file, below, in a text editor.

`C:/Program Files/Helicon/ISAPI_Rewrite3/httpd.conf`

2 The file lets you declare the target of the proxy and (optionally) a header that's used for SSO authentication. Everyone should add the proxy information. If you're using SSO, you must also add the SSO header. The two sections are displayed below:

IMPORTANT The SSO header must come before the proxy information.

```
## Change YourDomainName to the name of your network domain.
RewriteCond %{REMOTE_USER} YourDomainName\\(.*) [NC]
RewriteHeader SM_USER: .* %1 [NC,L]

## Change AtlasServerURL to the URL of the Atlas app server
RewriteBase /
RewriteRule ^PolicyAtlas(.+)$ http://AtlasServerURL:8080/PolicyAtlas$1 [NC,P,L]
```

SSO header

Proxy information

- `YourDomainName` is the name of the network domain that the Atlas application is part of.
- `AtlasServerURL` is the URL of the application server that hosts the Atlas application.

3 Save and close the file.

5.3 Configure SSO

The instructions for SSO configuration are provided in the HTTP-based SSO section of the next chapter, User Authentication. You must configure IBM Atlas Suite to use HTTP-based ("SiteMinder-like") SSO. *Don't* configure the system to use NTLM SSO, even though you're using NTLMv2.

For IIS, the settings that you'll use in the **`ssoConfig.properties`** file are:

```
sso.enabled=true
sso.header.name=SM_USER
sso.column.name=LoginID
sso.type=SM
```

5.4 Testing the Configuration

To test the connection between IIS and the Atlas application, log into a computer that can reach the IIS machine as a user who has an IBM Atlas suite account, and then open a web browser and go to this URL:

`http://IISServerURL/PolicyAtlas`

…where **`IISServerURL`** is the URL of your Windows IIS machine. You should see the following:

- If you're not using SSO, you'll see the **Log into Atlas Suite** page.
- If you're using SSO, you'll see the **My Atlas** page within the Atlas application.

If you don't see the login or **My Atlas** page, the connection isn't working. To troubleshoot, you can view the SSO headers by going to this URL:

`http://IISServerURL/PolicyAtlas/faces/pages/debug/debug.jsp`

6 User Authentication

This chapter tells you how to configure the system so it works with an external authentication system. It also tells you how to set the rules for passwords that are authenticated by the Atlas application.

- If you want to mediate access to the Atlas application through a Microsoft Internet Information Server, see the Interaction with Windows Internet Information Server (IIS) chapter, first. As you're configuring the IIS authentication, you'll be directed back to this chapter for Single Sign-On (SSO) configuration.
- If you're using an HTTP-based single sign-on system such as SiteMinder or WebSEAL, see HTTP-based SSO.
- If you're using NT LAN Manager (NTLM) see NTLM SSO.
- If you use LDAP for authentication, see the *LDAP Authentication* chapter of the **AIBM Atlas Suite Administrators Guide: Components** book.
- Although it's expected that most companies will use an external authentication system, it's possible to use the Atlas application for this task. To configure Atlas so that it enforces formatting rules for passwords and other authentication-related attributes, see the **LOGIN_MANAGEMENT** Component.

6.1 HTTP-based SSO

To use an HTTP-based SSO system, you must first configure the SSO product to send a message to the Atlas application when a user logs in. How you configure your SSO system depends on the software you're using; consult your SSO documentation for instructions.

The message that the SSO system sends to the Atlas application includes a parameter that identifies the logged in user. The parameter consists of a name and an authentication token in the form **`name=token`**; for example:

```
SM_USER=admin
```

The Atlas application takes the token (**`admin`** in the example) and looks for a Person account that has a specific attribute that matches that token. If it finds a match, the Person is allowed to log into Atlas.

To make this work, you need to know two things:

- You need to know the name of the parameter that the SSO system is going to send. The name of the parameter depends on your SSO system; consult your SSO documentation to discover the name. The default name for SiteMinder, as shown in the example, is **`SM_USER`**. The default for WebSEAL is (typically) **`HTTP_IV_USER`**.
- You need to know what the SSO system is going to send as the authentication token. Typically, the token is a login name, although, again, you can configure your system to send some other value. If you've seeded your SSO system with authentication tokens from an external system, you'll need to seed Atlas with the same tokens.

After you've determined what sort of authentication token the system is going to send, you need to tell Atlas which Person attribute it should compare the token to—we'll call this the "SSO token attribute". When designating the SSO token attribute, keep in mind that the attribute's value, across all Person accounts, must be unique. The suggested attributes, in rough order of preference, are:

- **`LoginID`**. Atlas forces this attribute to be unique, so the **`LoginID`** is a natural choice.
- **`PersonIdentifier`**. This attribute is designed to store unique, global identifiers that are read in from an external database through Atlas Extensions. When imported in this way, Atlas forces the **`PersonIdentifier`** value to be unique.
- **`PAField1`**-**`PAField5`**. Each Person account has five custom fields—**`PAField1`**, **`PAField2`**, and so on—that can be used for whatever purposes you want. Atlas never forces these attributes to contain unique values, but one of the benefits of using a custom field as the authentication token is that you can hide the field from users by unchecking the **Visible** checkbox in **Admin > Custom Fields**. Some enterprises demand that authentication tokens be hidden from users.

6.1.1 Configuring Atlas for SSO

After you've gathered the necessary information, do this:

1 Log into the Atlas application server platform and open **`C:/ATLAS/Properties/ssoConfig.properties`** in a text editor.

2 Look for these parameters:

```
sso.enabled=false
sso.header.name=SM_USER
sso.column.name=LoginID
sso.type=SM
```

3 Set the parameters' values as shown below:

```
sso.enabled=true
sso.header.name=ssoParameterName
sso.column.name=ssoTokenAttribute
sso.type=SM
```

`ssoParameterName` and ***`ssoTokenAttribute`*** are the parameter name and SSO token attribute that you've chosen to use. Leave **`sso.type`** set to **`SM`** (which stands for "SiteMinder-like").

The default settings, shown in the previous step, are typical for SiteMinder. A typical configuration for WebSEAL might look like this:

```
sso.enabled=true
sso.header.name=HTTP_IV_USER
sso.column.name=PersonIdentifier
sso.type=SM
```

4 Save and close the file.

5 If you deployed the Atlas Extensions application on a separate platform, copy the `ssoConfig.properties` file into the `C:/ATLAS/Properties` directory of that other platform.

6.1.2 Create an Initial SSO Account in Atlas

Before you switch over to your SSO system (by restarting the application server), you must create at least one Person account that can be authenticated by SSO, otherwise you won't be able to log into the Atlas application. The account must have System Administration privileges.

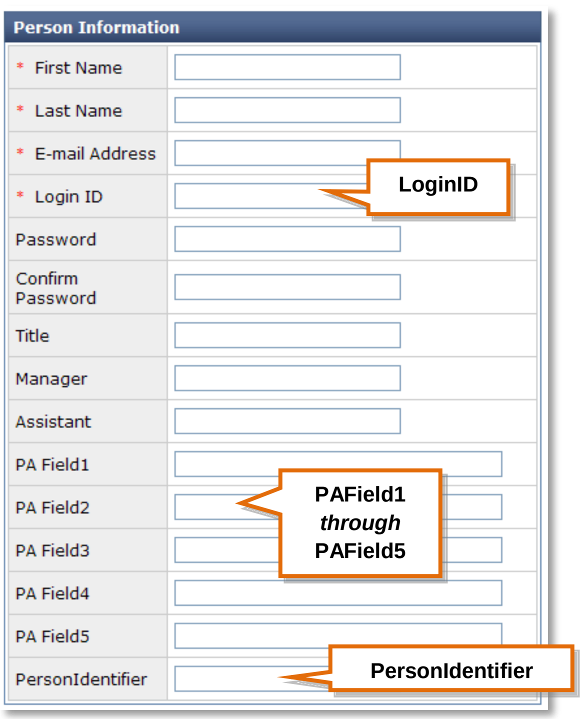
NOTE If you're using an SSO token attribute other than `LoginID`, you should be able to modify the default System Administrator account (**admin**) rather than having to create an entire new one—simply set the SSO token attribute appropriately. Furthermore, if you *are* using `LoginID` and you have an account named **admin** in your SSO system, you can use the Atlas **admin** account as is, without having to make any changes.

To create the first SSO user, do this:

1 Go to **Admin > Persons**.

2 Click **New Person**.

3 Fill in the Person attribute values as needed, making sure you set the SSO token attribute properly. The correspondences between the SSO token attributes and the Person attributes that are presented in the Atlas UI are shown below:



4 In the **Resource Chooser** panel on the right, check the checkbox next to the **Corporate (US)** Organization. This is the default Organization object that is typically used to represent your entire organization.

5 Click **Add & Assign Role** at the top of the **Resource Chooser** panel.

6 **Corporate (US)** will be added to the **Assigned Policy Atlas Roles by Organization** list near the bottom of the page. Check the item's checkbox, then open the **Role** dropdown menu and select **System Administrator**.

7 Click **Save & Close** at the top of the page.

After you restart the application server, your SSO system will be used for Atlas login authentication. You'll be able to log in using the Person account you just created.

6.2 NTLM SSO

To enable NTLM, you have to edit a configuration file and create a user account that corresponds to an account that exists on your Active Directory domain controller.

6.2.1 Edit the Single Sign-on Configuration File

1 Log into the Atlas application server platform and open this file in a text editor:

`C:/ATLAS/Properties/ssoConfig.properties`

2 Set the parameters listed below (*don't* modify parameters that aren't listed here):

- `sso.enabled`. Set this to `true`; it tells Atlas that you're using the single sign-on feature.
- `sso.type`. Set this to `NTLM`; this is the type of single sign-on that you're using.
- `jcifs.http.domainController` identifies the Active Directory domain controller. The value can be a hostname or an IP address.
- `jcifs.smb.client.username` and `.password` identify an account that already exists on the Active Directory domain controller.

```
sso.enabled=true
sso.type=NTLM
…
jcifs.http.domainController=domainControllerHostOrIP
…
jcifs.smb.client.username=activeDirectoryAccountName
jcifs.smb.client.password=activeDirectoryAccountPassword
```

3 Save and close the file.

4 If you deployed the Atlas Extensions application on a separate platform, copy the `ssoConfig.properties` file into the `C:/ATLAS/Properties` directory of that other platform.

6.2.2 Create an Atlas User

You have to create an account that corresponds to the Active Directory account that you used as the value of the `jcifs.smb.client.username` parameter.

1 Go to the **Admin > Persons** page and click **New Person**.

2 In the **Person Information** form, fill in the required information. Make sure the **Login ID** field matches the name you used as the value of the **`jcifs.smb.client.username`** parameter.

3 In the **Resource Chooser** panel on the right, check the checkbox next to the **Corporate (US)** Organization. This is the default Organization object that is typically used to represent your entire organization.

4 Click **Add & Assign Role** at the top of the **Resource Chooser** panel.

5 **Corporate (US)** will be added to the **Assigned Policy Atlas Roles by Organization** list near the bottom of the page. Check the item's checkbox, then open the Role dropdown menu and select System Administrator.

6 Click **Save & Close** at the top of the page.

After you restart the application server, NTLM will be used for Atlas login authentication.

6.3 LDAP

Although the Atlas application contains its own user authentication system, most large companies want or need to use their own system for authentication. This chapter tells you how to configure the **LDAP Server Template** Component so Atlas can communicate with your Lightweight Directory Access Protocol (LDAP) server.

If you're using an LDAP system, you must configure the LDAP Server Template Component. See the *LDAP Authentication* chapter in the **IBM Atlas Suite Administrators Guide: Components** book for details.

7 Atlas Reports Configuration

This chapter tells you how to configure the Atlas Reports application. It should be used by an Atlas administrator. To follow the instructions in this chapter, you'll need the following information:

- The name of the schema owner database account (**`PSSAPL`**).
- The hostname (or IP address) and port number of the application server that hosts Atlas (**`AtlasServerHost`** and **`AtlasServerPort`**).
- The hostname (or IP address) and port number of the application server that hosts Atlas Reports (**`ReportsServerHost`** and **`ReportsServerPort`**).

There are two Atlas Reports configuration files, as listed and described in the following sections. You should have copied these files onto the Atlas Reports platform when you configured the application server.

In addition to modifying the configuration files, you need to tell the main Atlas application how to find Atlas Reports by setting the Parameters in the **REPORTING** Component

7.1 General Configuration

FILE: **`ATLAS`**`/Properties/AtlasReportConfig.properties`

Property
`logDirectory=<PATH_TO_BIRT_LOG_DIRECTORY>` **`logLevel=INFO`**
Atlas Reports is built on top of the BIRT Reporting Engine. These two properties set the directory that BIRT uses to store its log files, and the granularity of the information that's logged. The directory needn't already exist; the name of the log file that BIRT creates is: **`ReportEngine_`*`datetime`*`.log`** The log levels are listed here in order of decreasing amounts of information: • **`FINEST`** (most info) • **`FINER`** • **`FINE`** • **`CONFIG`** • **`INFO`** • **`WARNING`** • **`SEVERE`** (least info) • **`OFF`** (no info)

Property
`report.runtime.mode=Standalone`
If you're testing the system, set this to **Standalone**. When you deploy your system in a production environment, set it to **Integration**.
`auth.server.url=http://AtlasServerHost:AtlasServerPort/PolicyAtlas/srsbs?oper=SessionAndReportInformation`
This is the URL of the applet that authenticates report users. You must set the host and port portions of the URL so that it points to the application server that hosts Atlas. The default port numbers are: • WebLogic: 7001 • WebSphere: 9080 • JBoss: 8080
`report.server.url=http://ReportsServerHost:ReportsServerPort/AtlasReports/frameset`
This is the URL of the applet that generates reports. You must set the host and port portions of the URL so that it points to the application server that hosts Atlas Reports.
`log4j.ATLAS_REPORTS.file=<PATH_TO_ATLAS_REPORTS_LOG_FILE>` `log4.ATLAS_REPORTS.logLevel=DEBUG`
These two properties set the location of the log4j log file that Atlas Reports creates, and the granularity of the information that's logged. The file needn't already exist. Atlas Reports will create it for you. The log levels are listed here in order of decreasing amounts of information: • **TRACE** (most info) • **DEBUG** • **INFO** • **WARN** • **ERROR** • **FATAL** (least info)

7.2 Schema Name

FILE: `ATLAS/Properties/AtlasReportStrings.properties`

This file contains the name of the schema that the Atlas Reports application uses to access the database.

Property
`report.common.schemaname=PSSAPL`
The name of the schema that the Atlas Reports application uses to access the database. You must set the value to **PSSAPL**.

Property
`report.common.dbVendorName=ORACLE`
Identifies the database that you're using. Uncomment the property that identifies Oracle.

You should leave the rest of the properties as they are.

8 Atlas UI

This chapter looks at the Components that configure aspects of the Atlas application UI.

8.1 List and Table Sizes

The **UI_SETTINGS** Component contains Parameters that limit the sizes of the tables and menus that are presented in the Atlas UI.

8.2 Menu Population

A number of menus are populated with options that are listed in various Components. Most of these menus are specific to a particular module, and are described elsewhere in this document. The Components listed here populate menus that appear throughout the Atlas UI:

- **USSTATES** supplies options that represent the 50 U.S. states plus the District of Columbia. Each Parameter's name is a two-letter state abbreviation. The Parameter's value is the state's human-readable display name.
- **COUNTRIES** supplies options that populate the various country dropdown menus. Each Parameter name is an ISO 3166 two character country code. The Parameter's value is the human-readable country name.

9 My Atlas Profiles

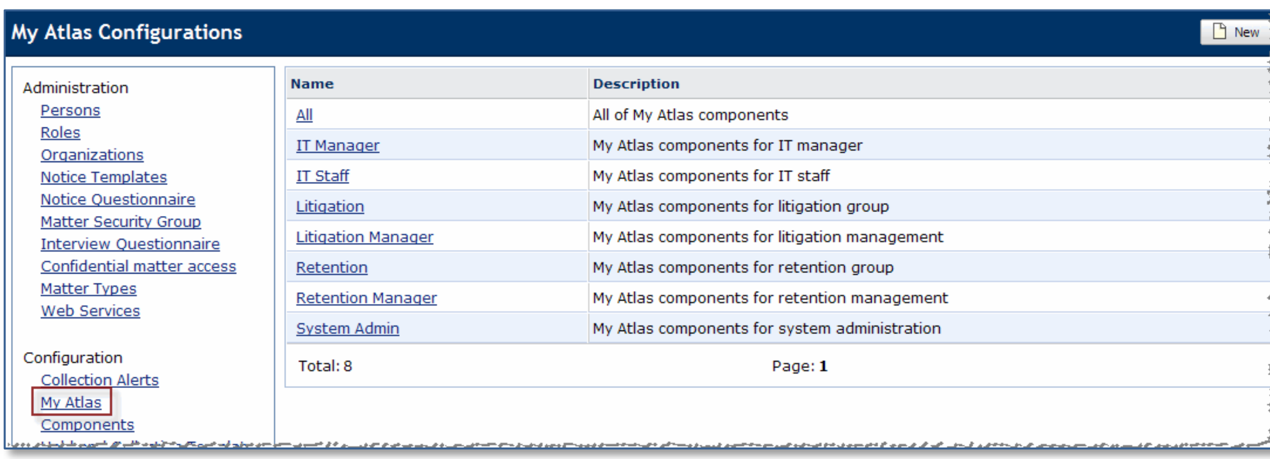
When a user logs into Atlas, the first page he or she sees is the **My Atlas** page. This is a dashboard that's populated with lists, tables, and bar graphs called *Trays*. Each Tray provides a particular set of information—a list of the Alerts the user has received, Retention Schedule approval requests that the user hasn't responded to, statistics about Legal Matters, and so on.

The set of Trays that a user sees is defined by his or her *My Atlas profile*. These profiles aren't assigned directly to individual users; instead, they're assigned to Roles. The user inherits the profiles of the Roles that he or she is given. For multiple Roles, the set of Trays is an accumulation of all of his or her Roles' profiles.

This chapter explains how to set up the My Atlas Profiles. The Trays themselves are described in the **IBM Atlas Suite Users Guide: My Atlas** book.

9.1 My Atlas Configuration Profiles

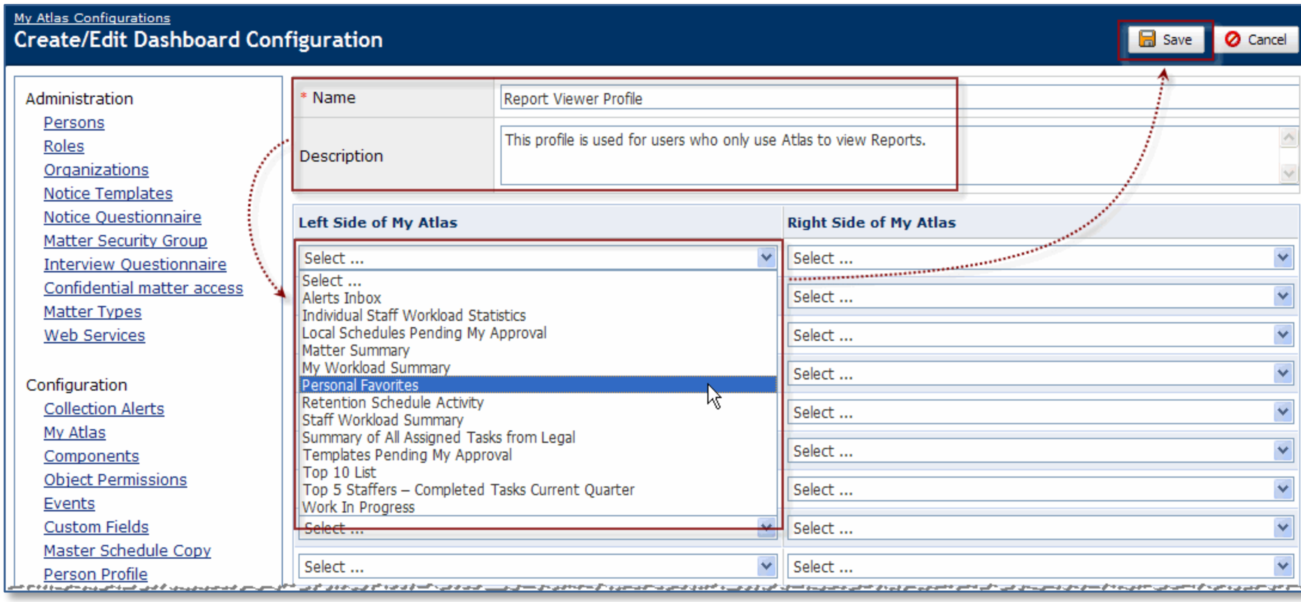
You access the My Atlas profiles through the **Admin > My Atlas** module, shown here with the default set of profiles:



The profiles assemble the Trays that are the most useful for the type of user that's described in the **Description** column.

9.1.1 Creating a My Atlas Profile

To create a new profile, click **New** on the **My Atlas Configurations** page. On the **Create/Edit Dashboard Configuration** page (below), give the profile a name and description, select the Trays that you want to include from the dropdown menus, and click **Save**:



Note:

- A profile can't include the same Tray more than once.
- You don't have to populate all the dropdowns.
- The Trays are distributed on the **My Atlas** page, top-to-bottom and left/right, just as you specify them here. The user can then log in and rearrange them directly on the **My Atlas** page by dragging-and-dropping.

9.1.2 Editing and Deleting a Profile

To edit or delete a profile, click the profile's name on the **My Atlas Configurations** page. You'll be taken to the **View Dashboard Configuration** page where you then select **Edit** (which takes you to the **Create/Edit Dashboard Configuration** page, shown above), or **Delete**.

To remove a Tray, reset the unwanted dropdown to **Select…**.

IMPORTANT	You can't delete a My Atlas profile that's been assigned to a Role, even if there are no Persons with that Role.

10 Custom Fields

The **Admin > Custom Fields** module lets you attach as many as five additional text attributes to some of the IBM Atlas Suite objects. The meanings of the attributes are up to you. For example, you can use a Person custom field to store a phone number, an attribute that's not included among the default set for a Person. You can also tell Atlas to make your custom fields a required part of an object's definition and to include the fields in the object's **Advanced Search** keyword search (for those objects that provide the facility).

The objects that take custom fields, grouped by topic, are:

Persons and Organizations

- Person
- Organization (this is called **OrgUnit** in the **Custom Fields** module)

Data Sources

- Data Source (**DataSource**)
- Data Source Data Management (**DataSourceDataManagement**)
- Data Source Discovery (**DataSourceDiscovery**)
- Data Source Type (**DataSourceType**)

Legal Matters

- Matter

Schedules

- Master Schedule (**PolicyTemplate**)
- Local Schedule (**PolicySchedule**)

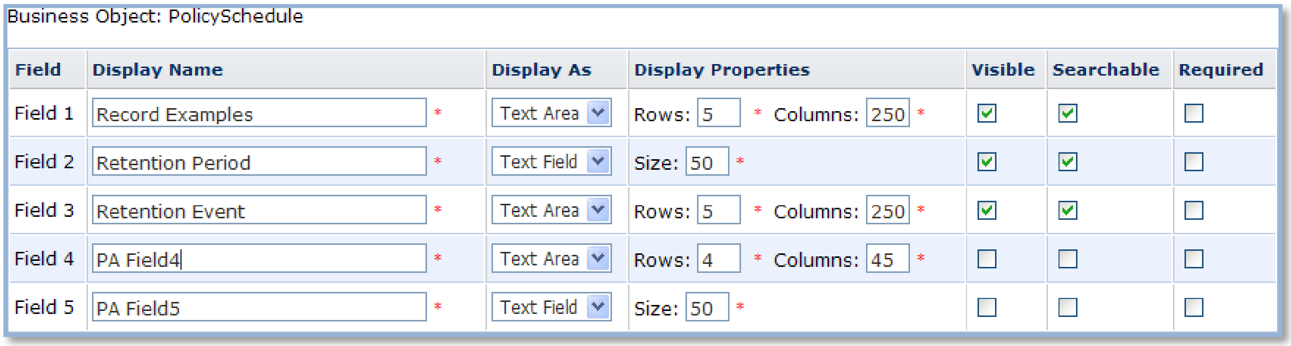
Law Library

- Citation
- Citation Requirements (**CitationRequirements**)
- GeoType (currently unused)
- GeoNode (currently unused)

Miscellaneous

- Project
- Action Item (**ActionItem**)

To add a custom field to an object, go to **Admin** > **Custom Fields** and select the object. You'll see the **Define Custom Fields** page:



The attributes on the page are:

Feature	Component > Parameter
Display Name	The label that's used when the custom field is displayed in the Atlas UI.
Display As	The type of input control that's presented to the user, either **Text Field** (a single line) or a **Text Area** (multiple lines).
Display Properties	If you're using a text field as the input control, the **Size** setting is the maximum number of characters the field will allow. For text areas, the **Rows/Columns** values are ignored. Text areas are limited to a maximum number of characters as defined by the object (either 2000 or 4000 depending on the object).
Visible	Whether or not the field is displayed in the user interface.
Searchable	Whether or not the field is included in a keyword search on the object's **Advanced Search** page. This only applies to objects that provide the **Advanced Search** facility:` • Master Schedules (**PolicyTemplate**) • Local Schedules (**PolicySchedule**) • Citations (including Citation Requirements) **NOTE** The custom fields for Citations and Citation Requirements are always included in the **Advanced Search** keyword search (for Citations), regardless of the **Searchable** setting. • Matters
Required	Whether or not the user must specify a value in the field when creating that type of object. **NOTE** The Data Source custom fields don't have a **Required** option. To declare that a Data Source custom field is required, you must define the field here (in **Admin > Custom Fields**) and then mark it as required in the **Admin > Data Source Maintenance** module. This applies to all four Data Source objects: Data Source, Data Source Data Management, Data Source Discovery, and Data Source Type.

11 Roles

A *Role* is the function that a user serves within an Organization. The most important aspect of a Role is that it has a set of *Permissions* that allow the user to view and modify certain business objects and perform certain functions. The Permissions that Atlas defines are described in the next chapter, Objects and Permissions.

A Role is assigned to a Person in the context of a particular Organization. For some objects, a Person can perform an action in an Organization only if he or she is assigned a Role that includes the corresponding Permission. For example, if you create the **Records Coordinator** Role with Permissions to create Local Schedules, and then assign Jack the **Records Coordinator** Role in the **Legal (Europe)** Organization, Jack can create Schedules in the **Legal (Europe)** Organization (and all of its sub-Organizations), but not in any other Organization.

11.1 Predefined Roles and Role Assignment Components

Atlas provides only a few predefined Roles (listed below); you have to create the other Roles that you need yourself, through the **Admin > Roles** module. Atlas also provides a set of *Role Assignment* Components (also listed below); these Components specify the Atlas Roles that can perform particular functions. For example, in order to be designated as the attorney for a Matter, a user must be given a Role that's listed in the **ATTORNEY** Component.

11.1.1 Predefined Roles

- A **System Administrator** has complete access to Atlas. This Role cannot be edited or deleted.
- A **Hold and Collection Plan Owner** can act as the owner of Structured Preservation/Collection Plans (within a Legal Matter).
- **IT Staff** can be assigned Structured Preservation/Collection Plan and Policy Distribution tasks. These users have access to the **My Tasks** module.
- A **Data Source Mapper** can create, edit, and deactivate a Data Source through the **Map > Data Sources** module.

11.1.2 Role Assignment Components

The Role Assignment Components are listed below with brief descriptions. For full descriptions, see **IBM Atlas Suite Administrators Guide: Components**.

11.1.2.1 Atlas Map

- **PERSON_DATA_PRIVACY_CONTROL** can view the Custom Fields that are attached to a Person account.
- **DS_APPROVER** can approve a request to create, update, or deactivate a Data Source.
- **DS_MAPPER** can create, edit, and deactivate a Data Source through the **Map > Data Sources** module.

11.1.2.2 Legal eDiscovery

- **ATTORNEY** can be designated as the Attorney for a Matter and can be assigned a Drop Box.
- **LEGAL ASSISTANT** can be designated as the Paralegal for a Matter and can be assigned a Drop Box.
- **LEGAL NOTICE APPROVER** can approve Notices and Plans.
- **LEGAL_POWER_USER** has special privileges when creating legal objects and generating legal reports.
- **NOTICE_RECIPIENT_REMOVER** can remove Persons from the recipient lists of all Holds and Virtual
- **COLLECTOR** can be designated as the conductor of a Collection in a Collection Log and can be assigned a Drop Box.
- **INTERVIEWER** can be designated as the conductor of an Interview in an Interview Log and can be assigned a Drop Box.
- **TRANSACTION_WORK_ASSIGNOR** can assign other Atlas users to be a Structured Plan Owners.
- **CONTENT_DISPOSAL_REQUESTER** can request that a Matter's documents be deleted.
- **CONTENT_DISPOSAL_APPROVER** can approve or reject requests to delete a Matter's documents.
- **CONTENT_DISPOSAL_SUBSCRIBER** is sent Alerts when a Disposal Request is approved and cancelled, and when a set of documents are about to be deleted.

11.1.2.3 Retention Management

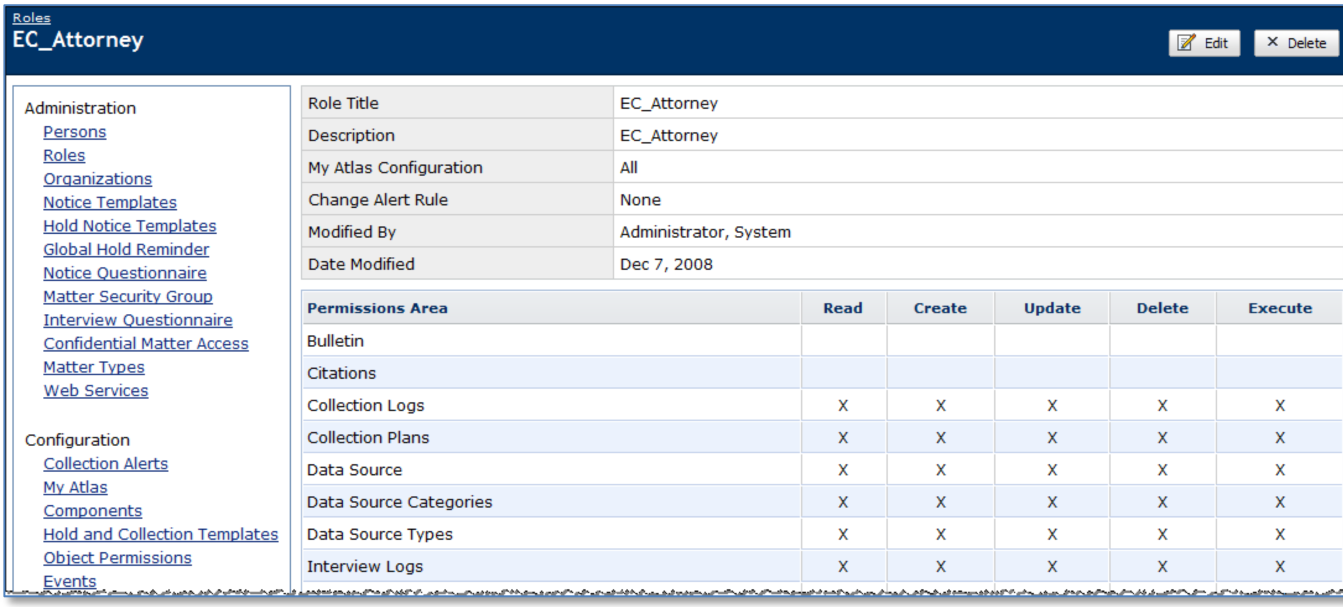
- **RECORDS CO-ORDINATOR** can act be designated as the Records Coordinators for Local Schedules and Projects.
- **AWF_ADMIN_ROLE** receives a notification when an approval request for a Retention Schedule has expired.
- **AWF_APPROVAL_ROLE_1** and **AWF_APPROVAL_ROLE_2** can approve Schedules.

11.1.2.4 Miscellaneous

- **ERM_ROLES** can create the distribution list for a bulletin (the **Communications** tab).
- **ROLE_USEDIN_ORG_WITH_OUT_MEMBERS** is listed as the "rogue Organization" contact in the **Organization Without Members** report.

11.2 Viewing Role Details

To view a Role, go to the **Roles** module and select a Role from the list. You're taken to the Role's details page:

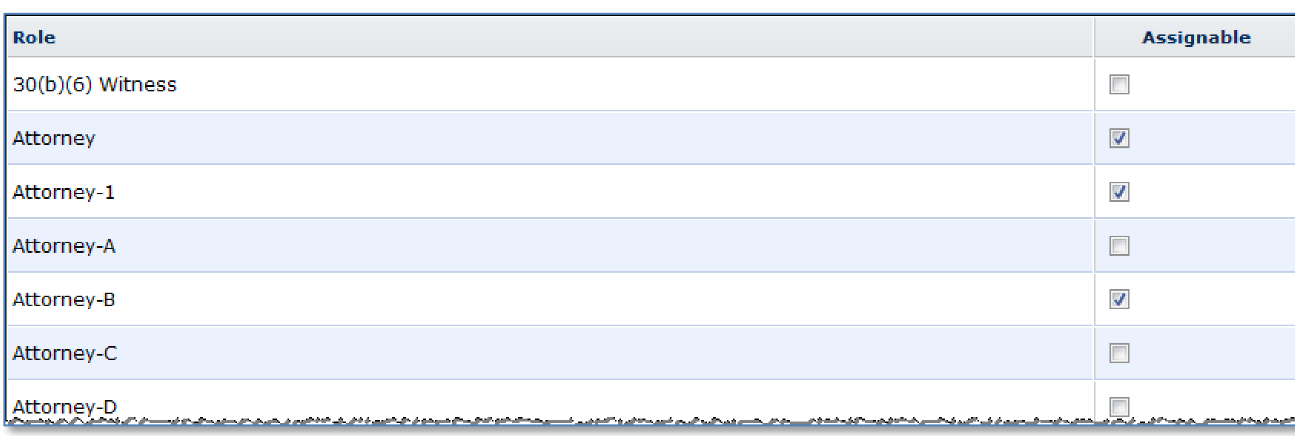


Role Title	EC_Attorney
Description	EC_Attorney
My Atlas Configuration	All
Change Alert Rule	None
Modified By	Administrator, System
Date Modified	Dec 7, 2008

Permissions Area	Read	Create	Update	Delete	Execute
Bulletin					
Citations					
Collection Logs	X	X	X	X	X
Collection Plans	X	X	X	X	X
Data Source	X	X	X	X	X
Data Source Categories	X	X	X	X	X
Data Source Types	X	X	X	X	X
Interview Logs	X	X	X	X	X

Most of the fields are self-explanatory; these require a bit more explanation:

- **My Atlas Configuration** is one of the Atlas Profiles that's defined in the **My Atlas** module. See the My Atlas Profiles chapter.
- **Change Alert Rule** is one of the rules defined in the **Change Alert Rules** module. The rule determines what sorts of changes trigger an Alert; for example, you can define a Role that receives an Alert when a Person record is modified.
- **Permissions Area** is a list of the Role's Permissions for various objects. The Permissions are listed and described in the next section.
- The **Role/Assignable** table at the bottom of the page (shown below) specifies the Roles that users with this Role can assign to other users (within the same Organization or sub-Organization, explained after the illustration). This only applies to Roles that include **System Administration** or **Organization System Administration** Permissions *and* **Users** Permissions.



Role	Assignable
30(b)(6) Witness	☐
Attorney	☑
Attorney-1	☑
Attorney-A	☐
Attorney-B	☑
Attorney-C	☐
Attorney-D	☐

For example, let's say that within the **Attorney** Role, you mark **Attorney** and **Paralegal** as **Assignable**. If you assign the **Attorney** Role to Jack in the **Legal** Organization, then:

- If Jack has **System Administration** Permission he can assign the **Attorney** and **Paralegal** Roles to anyone in his own Organization or sub-Organization.
- If Jack has **Organization System Administration** Permission he can assign the **Paralegal** Role to anyone in his Organization or sub-Organization, but he can only assign **Attorney** (his own Role) to users in sub-Organizations.

NOTE A User with the **System Administrator** Role can assign any Role to users in any Organization.

12 Objects and Permissions

The tables in this chapter list and describe the Permissions that you can assign to Roles. Each type of Permission comprises five activities for a particular object: **Create**, **Read**, **Update**, **Delete**, and **Execute**. The meanings of these activities are usually straightforward. For example, if a Role has **Delete** permission for **Matter** objects, users with that Role can delete Matters. If an activity for a particular object isn't obvious, it's noted in the table's **Description** column.

12.1 System Administrators

The Permissions in this section control the accessibility of the modules in the **Admin** tab. They're assigned to System Administrators.

There are two types of Administrators: the System Administrator and the Organization System Administrator. You designate a user as an Administrator by granting them **System Administration** (**SA**) or **Organization System Administration** (**OSA**) permissions. The differences between the two are:

- A System Administrator has (potentially) access to all of **Admin** modules; Organization System Administrators can access the modules in the **Administration** section, only. In both cases, an Organization System Administrator can only create, modify, and delete Organizations and Persons who are in the user's own Organization or sub-Organization.

IMPORTANT	Also see the **OSA_ALLOW_OTHER_ORG_MEMBERSHIP_EDIT** Component, which allows an OSA to modify Members (Persons without Roles) anywhere in the Organization hierarchy).

- A System Administrator can assign his or her own Role to some other user who's in the same Organization (and sub-Organizations); an Organization System Administrator can only assign his/her own Role to users who are in sub-Organizations.

In a typical deployment, only the default System Administrator Role is given **System Administration** permissions. Individual business units then create Roles that are given Organization System Administration permissions and assign these Roles to users who act as limited administrators for the unit.

The rest of the Administrator permissions control access to (primarily) the **Admin > Administration** modules. They all require either **System Administration** or **Organization System Administration** permission. For example, if you want a user to be able to access the **Admin > Matter Types** module, you must grant the user's Role both **Matter Type** and either **System Administration** or **Organization System Administration** permissions.

12.1.1 SA and OSA

	Description	R	C	U	D	E
System Administration	Designates the Role as a System Administrator • You must set all five access types (**Read**, **Create**, **Update**, **Modify**, and **Delete**). Setting a subset can cause unpredictable behavior.	X	X	X	X	X
Organization System Administration	Designates the Role as an Organization System Administrator • You only need to grant **Read** access. The other access types are controlled by the additional permissions (**Organizations**, **Roles**, **Users**, and so on).	X	-	-	-	-

12.1.2 Administration Module

IMPORTANT	The permissions listed in the following table require either **System Administration** or **Organization System Administration** permission.

	Description	R	C	U	D	E
Organizations	Grants access to **Admin > Organizations**.	X	X	X	X	-
Roles	Grants access to **Admin > Roles**. • You should never create a Role that has **Organization System Administration** plus **Roles (Update)** Permission. A user with this combination of Permissions could modify any Role in the system, including his or her own Role.	X	X	X	X	-
Users	Grants access to **Admin > Persons**.	X	X	X	X	-
Matter Security Group	Grants access to **Admin > Matter Security Group**.	X	X	X	X	-
Matter Type	Grants access to **Admin > Matter Types**.	X	X	X	X	-
Notice Templates	Grants access to **Admin > Notice Templates**.	X	X	X	X	-
Hold Notice Templates	Grants access to **Admin >Hold Notice Templates**.	X	X	X	X	-
Global Hold Reminder	Grants access to **Admin > Global Hold Reminders**.	X	X	X	X	-
Notice Questionnaire	Grants access to **Admin > Notice Questionnaire**.	X	X	X	X	-
Interview Questionnaire	Grants access to **Admin > Interview Questionnaire**.	X	X	X	X	-
Manage Applications	Grants access to **Admin > Web Services**.	X	X	X	X	-

IMPORTANT	The permissions listed in the following table require **System Administration** permission.

	Description	R	C	U	D	E
Reports	Grants access to **Admin > Manage Reports** and **Manage Report Groups**.	X	X	X	X	-
Ach Transaction Query Template	Grants access to **Admin > Hold and Collection Templates**.	X	X	X	X	-

12.2 Business User Permissions

The permissions in the section are given to normal (non-Administrator) business users. They control access to Matters, Retention Schedules, the modules in the **Map** tab, and so on.

12.2.1 Atlas Map

These permissions control access to the modules in the **Map** tab.

	Description	R	C	U	D	E
Map	Displays the **Map** tab. To grant access to the Map's modules, you need to combine **Map (Read)** with the appropriate **Data Sources**, **Users**, and **Organizations** permissions, listed below.	X	-	-	-	-

IMPORTANT The rest of the permissions in this section require **Map (Read)** permission.

	Description	R	C	U	D	E
Organizations	Grants access to **Map > Organizations**.	X	X	X	X	-
Users	Grants access to **Map > Persons**. **NOTE** You don't need **Users** permissions to assign Persons as Attorneys, Data Source Stewards, Notice Recipients, and so on.	X	X	X	X	-
Data Source	Grants access to **Map > Data Sources > Catalog** and **Catalog Management.** • To request new Data Sources from the **Local Schedules** and **Matters** modules you must have **Data Source (Create)** permission (as well as the appropriate Local Schedules and Matters permissions).	X	X	X	X	-
Data Source Categories	Grants access to **Map > Data Sources > Categories**.	X	X	X	X	-
Data Source Types	Grants access to **Map > Data Sources > Types**.	X	X	X	X	-
Data Governance Metrics	Grants access to **Map > Data Sources > Data Governance Metrics**. • Only **Read** permission is used. • Requires **Data Source (Read)** (in addition to **Map (Read)**).	X	-	-	-	-

	Description	R	C	U	D	E
Ach Transaction Query Template	Grants access to **Map > Data Sources > Preservation and Collection Plan Templates**. • **Update** permission is required.	X	X	X	X	-

12.2.2 Legal eDiscovery

The permissions in the section control access to the objects that are involved in the legal eDiscovery process: Matters, Requests, Notices, and so on.

	Description	R	C	U	D	E
Matters	Displays the **Matters** tab and grants access to the **Master List** and **Documents** tabs. For access to other Matter objects (Requests, Notices, Logs, and so on) you must add the other permissions listed in this section. • **Read** lets you export documents and initiate and approve document disposition (given the proper disposition role assignments as set through the **CONTENT_DISPOSAL_REQESTER** and **CONTENT_DISPOSAL_APPROVAL** Components). • **Delete** lets you deactivate Matters. • **Execute** lets you close and reopen Matters. • Any Role that is part of a Matter Security Group must be given (at least) **Matters (Read)** permission. • To view the list of Reports on the Matter **Detail** page, you also need **Reports (Read)** permission.	X	X	X	X	X

IMPORTANT The rest of the permissions in this section require **Matters (Read)** permission.

	Description	R	C	U	D	E
Matter Access Control List	Grants access to a Matter's Matter Access List (through the **Matter Access** button). • To add users to the list you must have **Create** and **Update** permission. • To remove users from the list you must have **Delete** permission.	X	X	X	X	-
Requests	Grants access to a Matter's Requests. • To create a Notice or Plan (of whatever type), you must have **Request (Read)** permission. • **Update** lets you mark Requests as **Complete**. • **Delete** lets you deactivate Requests.	X	X	X	X	-

	Description	R	C	U	D	E
Notices	Grants access to a Matter's Hold and Collection Notices. • **Create** requires **Requests (Read)**. • To send a copy of a Notice to yourself (through the **Send Me** button) you need **Update** or **Execute** permission. • **Execute** lets you publish Notices. • **Delete** lets you deactivate Notices.	X	X	X	X	X
Collection Plans	Grants access to a Matter's Self-Collection Plans. • Requires **Notices (Read)**. • **Create** is unused; Self-Collection Plan creation is controlled by **Notices (Create)**. • **Update** lets you mark Plans as **Complete** (by marking all of a Plan's Log entries as **Complete)**. To reopen a Log entry, and thus reopen the Plan, you need **Collection Logs (Update)** permission. • **Delete** lets you deactivate Plans.	X	-	X	X	X
Collection Logs	Grants access to a Matter's Collection Logs. • Requires **Notices (Read)**. • **Update** lets you reopen Log entries that have been marked as **Complete**. To mark an entry as **Complete**, you need **Collection Plans (Update)** permission. • You can't delete Log entries.	X	X	X		
Interview Plans	Grants access to a Matter's Virtual Interview Plans. • **Update** lets you mark Plans as **Complete**.	X	X	X	-	-
Interview Logs	Grants access to a Matter's Interview Logs. • Requires **Interview Plans (Read)**. • You can't edit or delete Interview Logs.	X	X	-	-	-
Transaction	Grants access to Structured Preservation and Collection Plans. • Requires **Notices (Read)**. • **Update** isn't used; **Create** includes update permission. • **Delete** isn't used. • **Execute** lets you publish and deactivate Plans.	X	X	-	-	X
My Tasks	Displays the **My Tasks** tab.	X	-	-	-	-

12.2.3 Retention Schedules

The permissions in this section provide access to Retention Schedules.

	Description	R	C	U	D	E
Templates	Grants access to **Schedules > Classification Library** (Master Schedules and Record Classes) and **Schedules > Project Templates**. • If Approval Workflow is enabled, **Update** lets you approve Master Schedules and Record Classes. • If Approval Workflow is disabled, **Execute** lets you approve Master Schedules and Record Classes.	X	X	X	X	X
Schedules	Grants access to **Schedules > Local Schedules**. • If Approval Workflow is enabled, **Update** lets you approve Local Schedules. • If Approval Workflow is disabled, **Execute** lets you approve Local Schedules.	X	X	X	X	X

12.2.4 Law Library

The permissions in this section provide access to the Law Library (i.e. Citations).

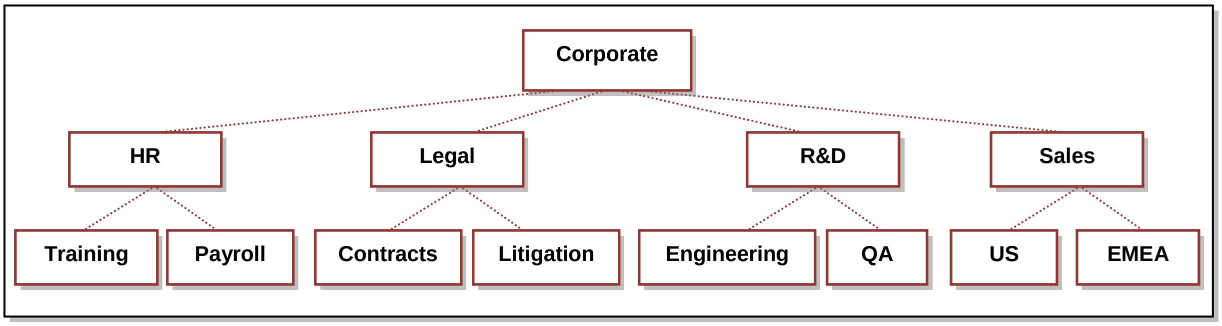
	Description	R	C	U	D	E
Citations	Displays the **Law Library** tab and grants access to Citations.	X	X	X	X	-

12.2.5 Miscellaneous

	Description	R	C	U	D	E
Projects	Displays the **Projects** tab and grants access to Projects.	X	X	X	X	-
Reports	Displays the **Reports** tab and displays the list of Reports on the Matter **Detail** page. • To view the Matter Reports, **Matters (Read)** is required.	X	-	-	-	-
Bulletin	Displays the **Communications** tab and grants access to Bulletins • **Execute** lets you publish Bulletins.	X	X	X	X	X
Cost Modelling	Displays the **Cost** tab and grants access to the IBM Atlas eDiscovery Cost Forecasting and Management data. • Only **Read** permission is used. **Read** lets you modify and save the cost profile for a Matter Type.	X	-	-	-	-

13 Organizations

An *Organization* represents a department, division, office, or other section of your company. Individual Organizations are organized into a hierarchy that's meant to reflect your company's actual departmental structure. Atlas creates a default Organization, named **Corporate**, that sits at the top of the hierarchy. All other Organizations inherit from **Corporate** in an expanding tree. Each Organization can inherit from only one parent:



Each Organization is populated with Persons, Data Sources, and other pertinent objects. The Organization can then be used as the basis for searching for a specific object. The proper construction and population of the Organization hierarchy might require guidance from your company's legal team and records management office.

In this chapter, we'll look at the relationship between Organizations and Persons, explain how to create and populate the hierarchy, tour the **Admin > Organizations** UI, look at an Organization's attributes, explain how to create and modify an Organization, and so on.

13.1 Organizations and Persons

Part of the construction of an Organization includes the establishment of the affiliations between your employees (represented as Persons accounts) and the Organizations that they belong to. Each Organization contains two types of affiliations:

- *Members*. A Member, as used here, is what one normally thinks of when describing a company's organizational structure: It's a person who's part of a division, business unit, department, and so on. The proper distribution of Members within Organizations is particularly important to Legal because of the ability to use Organizations to construct the Scope of a Legal Request. Organization Members can receive Hold and Collection Notices, respond to Virtual Interviews, upload collected documents, and so on. They can also receive Bulletins and Alerts (as email messages, only). When Members log into Atlas, the only tab they see is **My Holds**—they don't have permission to view, create, or modify business objects.
- *Users*. A User is a Person who has been given a Role in a specific Organization, and is expected to fulfill some business or administrative function for that Organization and its sub-Organizations. A single Person can be a User in more than one Organization, and can take on any number of Roles within the same Organization. When Users log into Atlas, they see the tabs that let them fulfill the designated function. A Records Manager would see the **Schedules** tab, for example; an Attorney would see **Matters**; a System Administrator sees **Admin**.

The same Person can be a Member of one or more Organizations, and a User in others. For example, a Record Manager might be listed as a Member of a specific Records Management department that's buried deep within the Organization hierarchy, and also act as the Records Coordinator User at the **Corporate** level and thus can make decisions, for the entire company, about how retention policies are created and stored.

13.2 Creating the Organization Hierarchy and Adding Persons

In most companies, the Organization hierarchy is populated and maintained by periodically importing data that's stored in the company's HRMS. There are two ways to import Organization data:

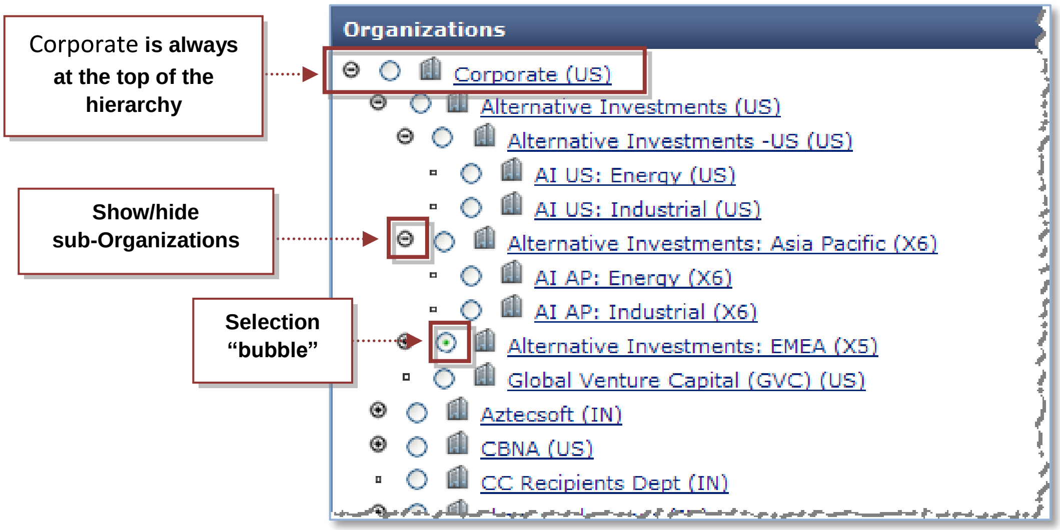
- Through Atlas Extensions, as described in **IBM Atlas Suite Administrators Guide: Atlas Extensions**.
- Through an **Organization** CSV file, as described in **IBM Atlas Suite Administrators Guide: Importing Data through CSV Files**.

Both methods let you create (and modify) Organizations and add members to them. The Atlas Extensions method, but not CVS, lets you delete (or, more precisely, *disable*) active Organizations.

You can also use the **Admin > Organizations** module to create and modify Organizations by hand, although for any large company this is a cumbersome and error-prone approach. If you use the UI to fine-tune the Organization data, be aware that if you're using either of the data-import methods, your manual changes could be overwritten the next time data is imported.

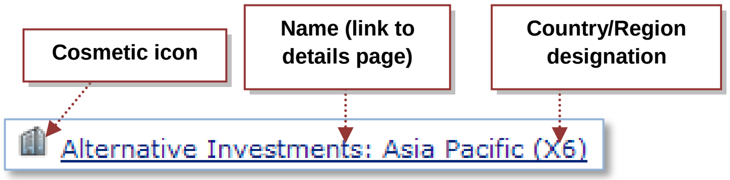
13.3 Organizations in the Atlas Administration UI

To view the Organization hierarchy, go to **Admin > Organizations**. The module displays the hierarchy in *tree view* mode:



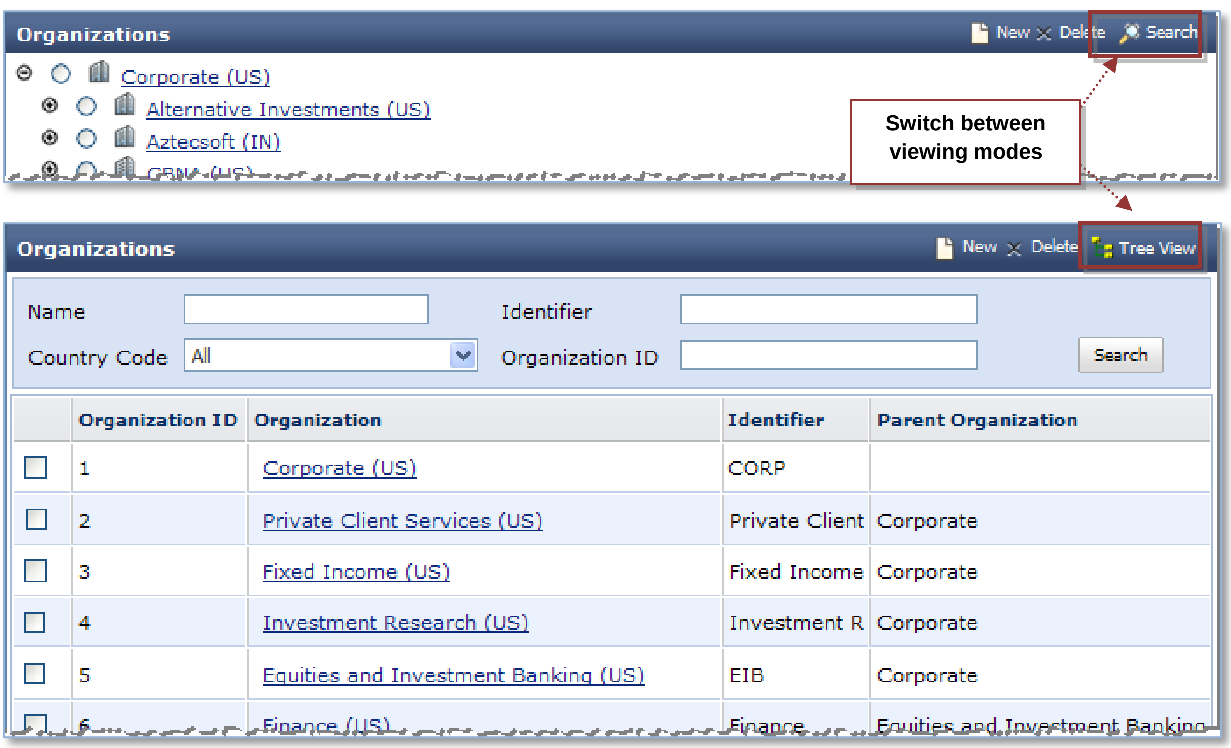
- As mentioned above, the **Corporate** Organization is always at the top of the hierarchy.
- The hierarchy is displayed as an indented list, where a "child" organization is indented beneath its "parent". You can hide and reveal a parent's list of children by clicking the **+/-** icon.
- To select an Organization (prior to deletion, for example) click its selection bubble.

Looking at an individual entry, we see this:



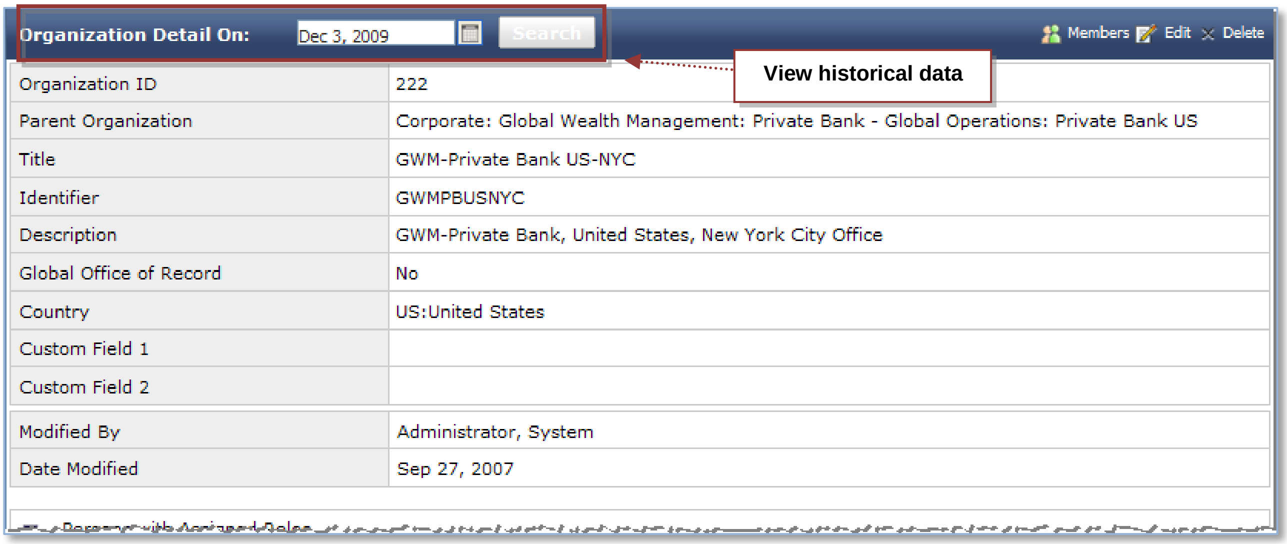
- The building icon to the left of the Organization's name is purely cosmetic. All Organizations display the same icon.
- The name of the Organization is a link that takes you to a page that lets you view and edit the Organization's details.
- Every Organization is created in the context of a country or region. The region's two-character code is presented in parentheses after the Organization's name. (**X6** represents the **Asia Pacific** region.)

To search for an Organization, click the **Search** button at the top of the page; this will take you to a page that sorts the Organizations into a flat list (*list view*) and that displays a set of search criteria. To return to the hierarchy tree, click the **Tree View** button:



13.3.1 The Organization Details Page

To view an Organization's details, you click the Organization's name in the hierarchy. This will take you to the **Organization Details** page:



By default, the **Organization Details** displays the current state of the Organization's attributes, and it lists (in the bottom half of the page) the Users who currently belong to the Organization, and the Data Sources and Local Schedules that have ever been related to the Organization, even if the relationship no longer exists (Members are listed on a different page, but the same current+historical rule applies there, as well).

You can view the data for a specific date (in the past, only) by selecting the date in the **Organization Detail On:** calendar. After you select a date, you have to click **Search** to refresh the page with the requested data.

13.3.2 Organization Attributes

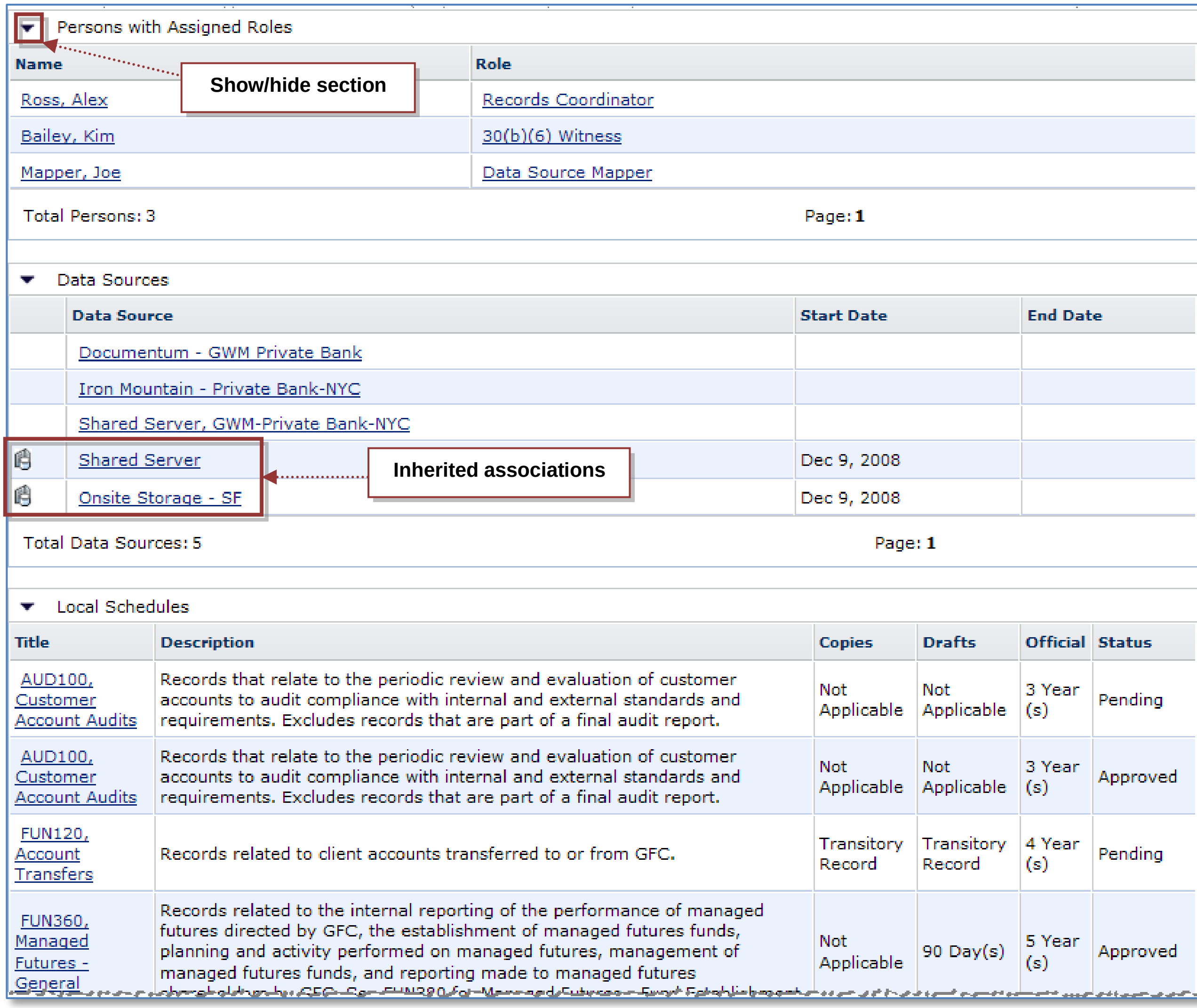
The table below lists and describes the Organization attributes that are displayed in the top half of the **Details** page:

Attribute	Meaning
Organization ID	This is a unique integer that's generated by the system when the Organization is created. You can't modify the **Organization ID**.
Parent Organization	The hierarchical "pathname" that leads to this Organization, starting with **Corporate** and ending with this Organization's immediate parent. The elements in the pathname are colon-separated. For example: **Corporate: HR: Personnel** The only Organization that doesn't have a parent is **Corporate**.
Title	The name of the Organization. The names of the Organizations within the same (immediate) parent must be case-insensitive unique. You should avoid using colons in an Organization's name; colons are used to separate Organization elements in the **Parent Organization** pathname construction.

Attribute	Meaning
Identifier	Not to be confused with **Organization ID**, this attribute is provided so you can tag each of your Organizations with an identifier that's meaningful to your company. If you import Organization data through Atlas Extensions, the **Identifier** values are required and must be unique across all Organizations. Note, however, that neither CSV ingestion nor creation though the Atlas UI impose these constraints on the attribute.
Description	An optional, human-readable description of the Organization.
Global Office of Record	Declares whether or not the Organization is always added to the **Office of Records** menu for Local Schedules. ("Global", here, means "applicable to any Local Schedule"—it's not a reference to geography.) Determining if an Organization should be marked as a global Office of Records is a business decision.
Country	The geographical location of the Organization. The country code is followed by the name of the country, as in **US:United States**. The list of candidate countries is provided by the **COUNTRIES** Component; you can add more countries (or regions) to the Component.
Custom Fields 1-5	You can add as many as five custom attributes to the Organization definition (the illustration shows two). To add custom attributes, edit the **OrgUnit** element in **Admin > Custom Fields**.
Modified By **Date Modified**	These two attributes provide the name of user who most recently modified the Organization, and the date of the modification.

13.3.3 Related Objects

The bottom half of the **Organization Details** page lists the objects (functional members, Data Sources, and Local Schedules) that are related to the Organization:



You can collapse a list by clicking its arrow toggle. The lists are described below:

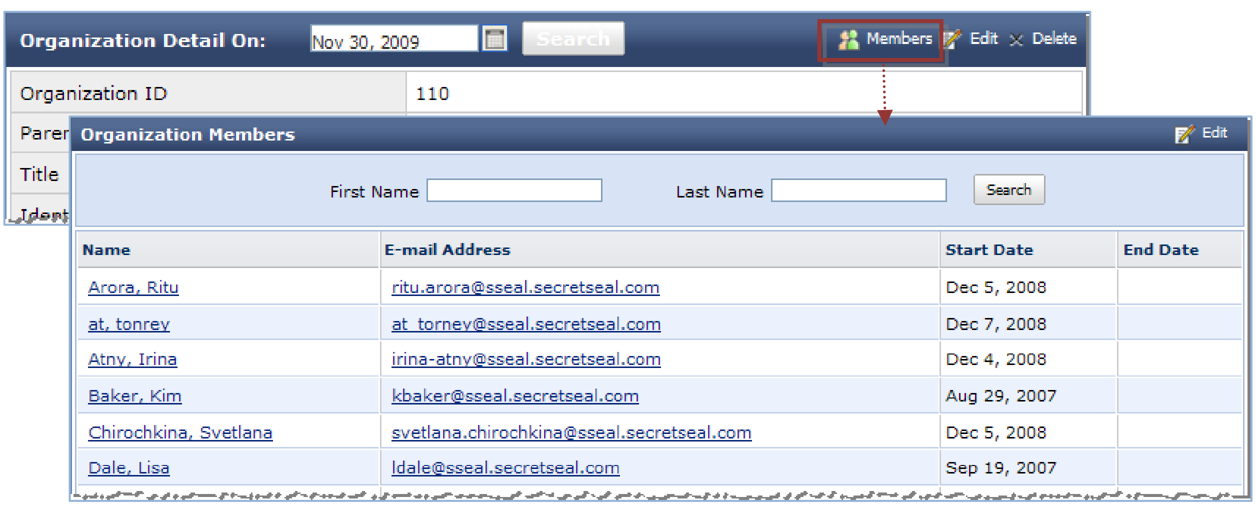
Object	Relationship
Persons with Assigned Roles	This is a list of the users who have been given Roles within the Organization.

Object	Relationship
Data Sources	An Organization can be associated with any number of Data Sources. The association means that the Data Source stores documents that are pertinent to the Organization. Although you can create (and sever) these associations through the **Admin > Organizations** module, this is typically a business task performed through **Map > Data Sources**. You can also associate a list of Organizations with a Data Source by importing a **Data Source** CSV file. If the left column contains a  icon, then the association is inherited from a parent Organization. If the icon is missing, the association was made directly to this Organization. You can't edit or remove an inherited association.
Local Schedules	An Organization can act as a Local Schedule's *Admin Organization*, and as its *Office of Records*. Assigning Organizations to these roles is a business task that's performed through the **Schedules > Local Schedules** module or by importing a **Local Schedule** CSV file. The **Local Schedules** list on this page displays the Local Schedules for which this Organization serves as the Admin Organization. It *doesn't* list the Schedules for which this Organization serves as the Office of Records.

In addition to these objects, an Organization can be added to the Scope of a Legal Request. When the Organization is added, so are all of its members and, optionally, its Data Sources. Adding Organizations to Scope is a business task that can only be performed through the **Matters > Requests** module.

13.3.4 Associated Members

To view Organization's list of Members (users without Roles), click the **Members** icon at the top of the **Organization Details** page. This will take you to the **Organization Members** page:



The list is filtered by the **Organization Detail On:** date setting.

13.4 Creating, Modifying, and Deleting Organizations

You can create and modify Organization through any of the three methods listed earlier: Through the **Admin > Organizations** module, through Atlas Extensions, or by importing an **Organization** CSV file (creation and modification only). This section describes the **Admin > Organizations** approach and points out any differences between the UI and import methods of creating and modifying Organization data.

13.4.1 Organization Permissions

To create, modify, or delete an Organization through the **Admin > Organizations** module, your Role must have the corresponding **Create**, **Update**, or **Delete** permission for the **Organization** object. (The **Execute** permission isn't used.) You *don't* need **Users** or **Data Source** permissions to modify an Organization's membership list or associations with Data Sources.

Organization permissions aren't needed to:

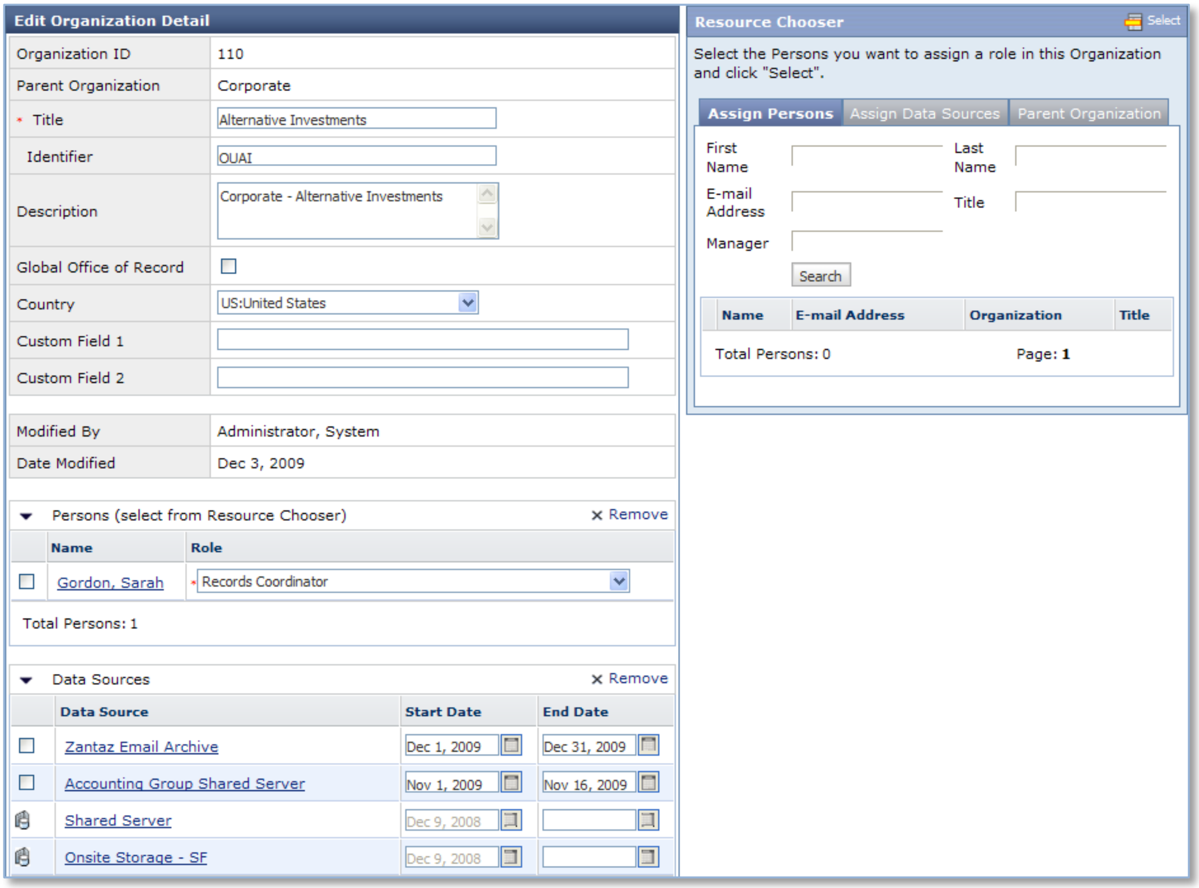
- Import Organization data through Atlas Extensions or an **Organization** CSV file.
- Change an Organization's membership list through **Admin > Persons**.
- Change its Data Source list through **Map > Data Sources**.
- Assign it as an Administration Organization or Office of Records through **Schedules > Local Schedule**.
- Add it to or remove it from the Scope of a Request.

13.4.2 Creating and Modifying an Organization

To create a new Organization, you have to select a parent Organization from the Organization tree or list on the main **Admin > Organizations** page, and then click **New**. This will take you to the **New Organization** page.

To edit an existing Organization, click its name in the Organization tree/list, and then click **Edit** on the **Organization Details** page. The **Edit Organization Details** page will appear.

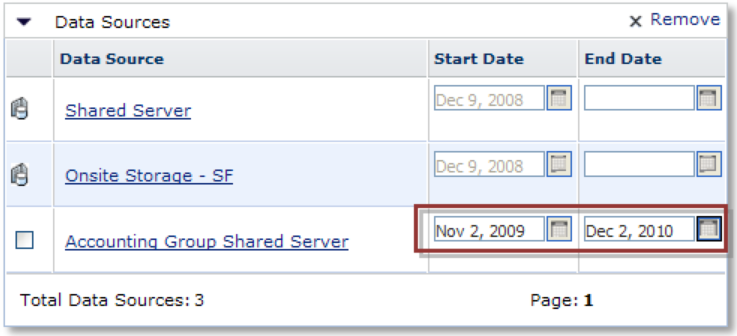
The **New Organization** and **Edit Organization Details** pages are essentially the same; here we see the **Edit Organization Details** page:



We've already looked at what the attributes and object lists mean. Here we'll point out some notable aspects of the tools that you'll use to create and modify Organizations.

- You add functional members, Data Sources, and set the parent Organization through the **Resource Chooser** on the right. To remove a member or sever the relationship with a Data Source, check the object's checkbox and click **Remove**.
- You can't create or sever the associations between Organizations and Local Schedules through this module.
- Although you *can* create and sever the associations between Organizations and Data Sources through this module, these operations are typically considered to be business tasks that are performed by an Atlas business user through the **Map > Data Sources** module.

- When you add a Data Source, you can set its start and end dates:



  These dates are used by the **Organization Detail On:** calendar to determine if the Data Source was associated with the Organization on a particular date. You can set the start and end dates to a time span in the past or in the future.

- You can't remove or edit the start and end dates of an inherited Data Source.

- A User also has a start and end date—but you can't set them here. To set the member's start and end date, you have to go to the **Admin > Persons** module.

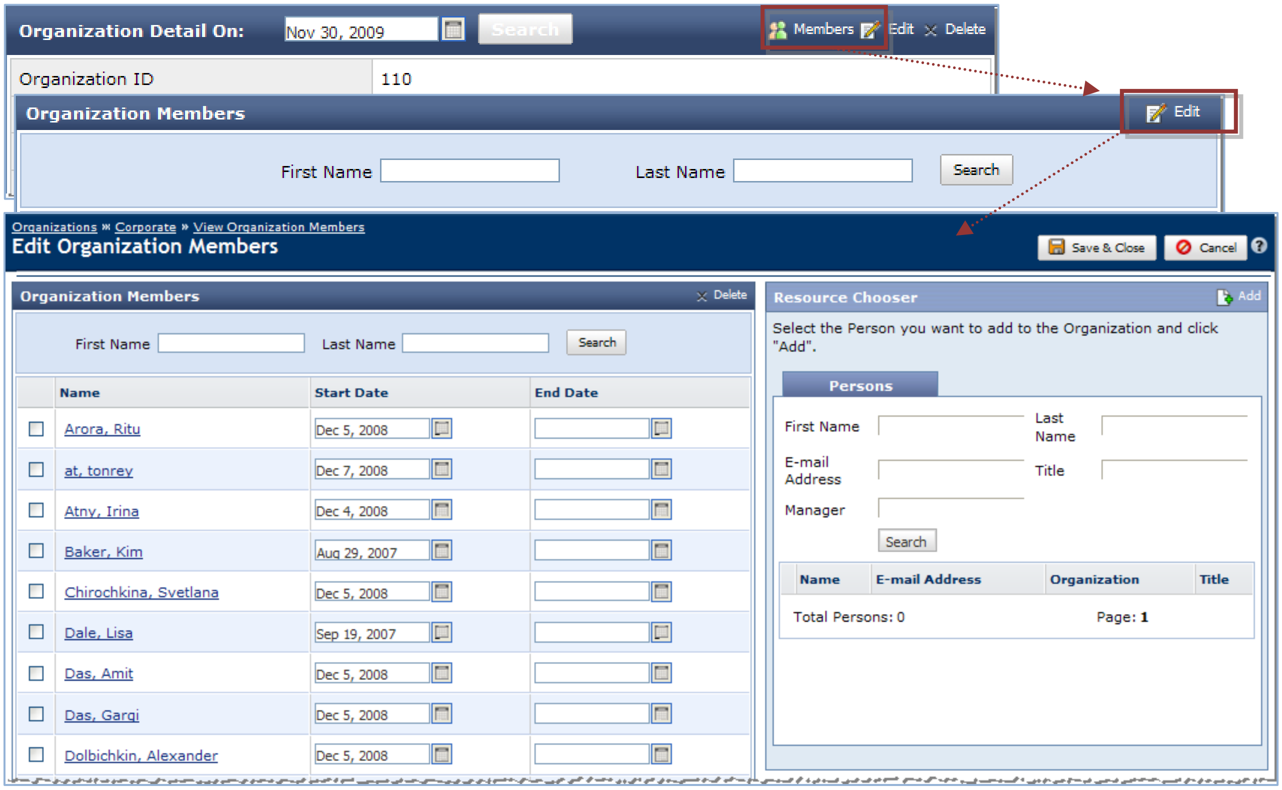
IMPORTANT	Currently, membership end dates must always remain in the future. If an end date expires, the Organization could become difficult to edit. When adding a member to an Organization you should leave the **End Date** field blank.

When you've finished creating or modifying the Organization, click **Save & Close**.

13.4.2.1 Modifying the Associated Members List

To modify the list of Members, click **Members** at the top of the **Organization Details** page, and then click **Edit** on the **Organization Members** page. This will take you to the **Edit Organization Membership** page.

NOTE	You can't jump straight from the **New Organization** or **Edit Organization Details** page to the **Edit Organization Membership** page. You have to save your changes and go back to the **Organization Details** page, first.



Use the **Resource Chooser** on the **Edit Organization Members** page to find and add Members. You can also set and modify the Member's start and end dates.

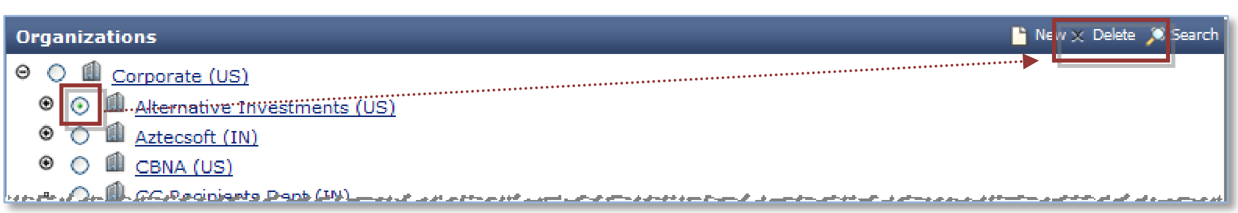
IMPORTANT	As mentioned above (in regard to Users), you should leave the **End Date** field blank.

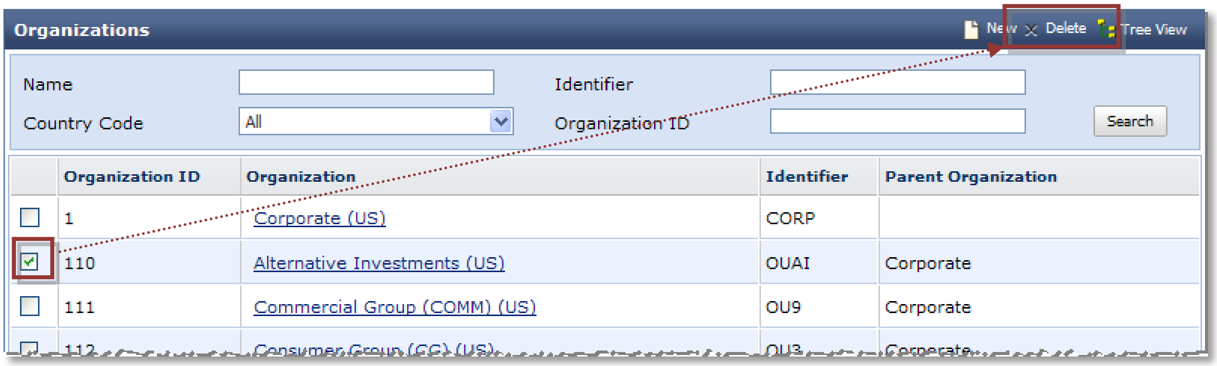
To remove a Member, check the Member's checkbox and click **Delete**.

13.4.3 Deleting an Organization

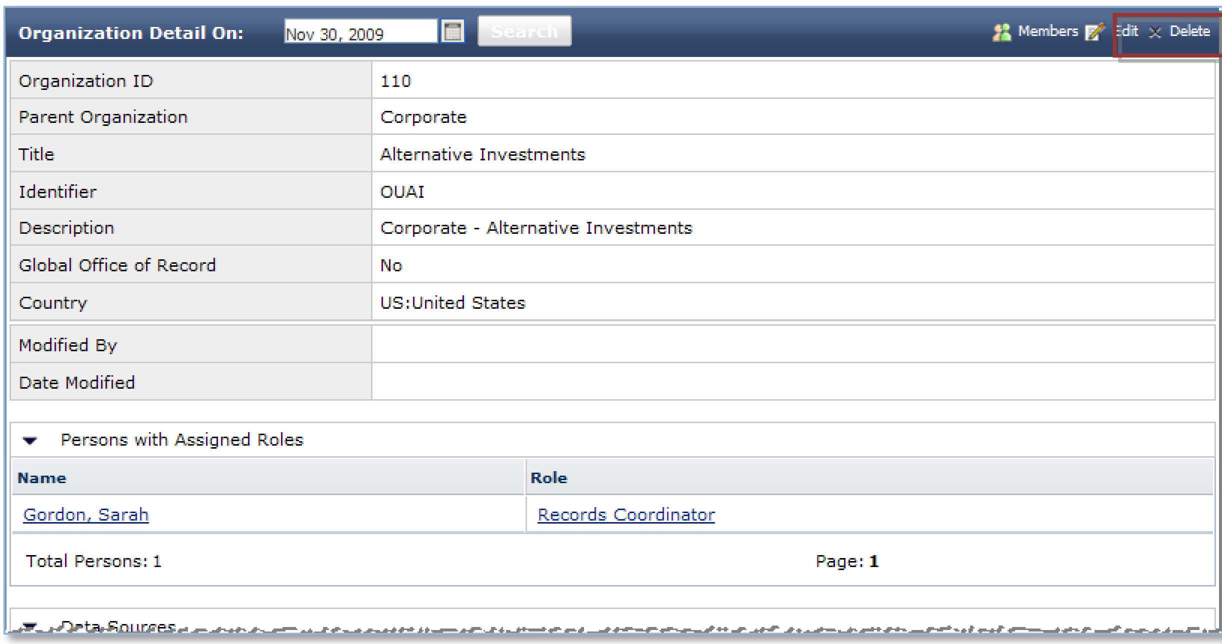
There are two ways to delete an Organization in the **Admin > Organizations** module:

- You can select it in the tree or list on the main page and click delete:





- You can click **delete** on the **Organization Details** page:



You can also delete an Organization through Atlas Extensions by setting the Organization's **Status** column to **DISABLED** and restore it by setting the **Status** to **Active.**

When you delete an Organization, all of its sub-Organizations are also deleted (or, technically, disabled). If you use the Atlas Extensions method to restore a disabled Organization, you have to restore the sub-Organizations individually—they're not restored automatically. When you restore an Organization, its membership lists and associations with Data Sources and Local Schedules are restored, as well.

If you delete an Organization, you won't be able to view its historical data. In general, you should try to avoid deleting Organizations.

NOTE The **Corporate** Organization can't be deleted.

14 Persons

A *Person* represents a person who's associated with your company; all of your company's employees should be represented by Person objects, as should non-employees such as outside counsel.

You can create Persons in one of the following ways:

- Through the **Admin > Person** module (as described in this chapter).
- Through Atlas Extensions, as described in **IBM Atlas Suite Administrators Guide: Atlas Extensions**.
- By importing a CSV file, as described in **IBM Atlas Suite Administrators Guide: Importing Data through CSV Files**.

A *User* is a Person who is assigned a Role in Atlas. A User can log into the Atlas application and perform operations.

A Person can also be a *Member* of an Organization, with no assigned Role. A Person without a Role in any Organization can't log into Atlas and has no operational privileges within the system.

You can associate a Person with one or more Organizations and assign one or more Roles to the Person in each of those Organizations.

When creating a Person, you can assign him or her a manager and an assistant. The manager relationship is used in the Legal Matters Notice escalation.

14.1 Viewing Person Attributes

To view the attributes of a Person, go to **Admin** > **Persons** and click the Person's name. The attributes are:

Field	Description
First Name	The first name of the Person.
Last Name	The last name of the Person.
Email Address	The email address of the Person.
Login ID	The Atlas login ID of the Person. The login ID is not case-sensitive.
Title	The title of the Person.
Manager	The name of the Person's manager.
Assistant	The name of the Person's assistant.
PAField1 **PAField2** **PAField3** **PAField4** **PAField5**	Custom properties that can be defined for Persons.

Field	Description
Assigned Roles by Organization	
Organization	The name of the Organization in which the Person has been assigned a Role.
Role	The Role assigned to the Person in the Organization. The effective dates (start and end dates) of the Person's association with the Organization are also displayed.
Member of Organizations	
Organization	The Organizations that the Person is a member of, but in which he or she has no Role. The effective dates of the membership are also displayed.

14.2 Creating a Person

You can create a Person in Atlas and assign the Person a Role in one or more Organizations so that the Person (as a User) can perform operations in Atlas. When a Person is associated with an Organization without being assigned a Role, the Person is only a Member of the Organization and cannot perform any operations in Atlas.

1 Click **Admin > Persons**.

2 On the Persons page, click **New Person**. The Person creation page is displayed.

3 Specify the Person information in the various fields. For field descriptions, see the table in the preceding section, Viewing Person Details.

4 To assign a Role in one or more Organizations:

  a In the Resource Chooser, click the **Organizations** tab.The Organizations configured in the system are displayed.

  b Select one or more check boxes for the Organization(s) in which you want to assign Roles to the Person, and click **Add & Assign Role**. The selected Organizations are displayed in the Assigned Roles by Organization tray.

  c Select the Role from the list in the **Role** column of the tray.

  d `(Optional)` In the **Start Date** and **End Date** columns of the tray, specify the effective dates of the Role in the Organization.

5 To assign Organization membership (without a Role):

  a In the Resource Chooser, click the **Organizations** tab.

  b Select one or more check boxes for the Organization(s) with which you want to associate the Person, and click Add.The selected Organizations are displayed in the Member of Organizations tray.

  c (Optional) In the Start Date and End Date columns of the tray, enter the effective dates of the Person's membership in the Organization.

6 To assign a manager or an assistant:

  a In the Resource Chooser, click the **Employee** tab. The names of Persons available in Atlas are displayed.

  b Select the corresponding check box and click **Select Manager** or **Select Assistant** to add the selected Person as the manager or assistant of the Person you're creating. The selected Person is displayed in the respective field.

7 Click **Save & Close**.

14.3 Deleting a Person

When you delete a Person from, the Person is marked **Inactive**. An **Inactive** User can no longer log into Atlas. To delete a Person:

1 Click **Admin** > **Persons**.

2 On the Persons page, click the name of the Person you want to delete. The Person detail page is displayed.

3 Click **Delete**.

4 Click **OK** to confirm the deletion.

IMPORTANT	The **System Administrator** User is vital to the working of Atlas Suite and must not be deleted.

15 Data Source Maintenance

Data Source Maintenance (creation, modification, and deletion) is subject to an approval workflow: A user can request the creation of a new Data Source, for example, but the Data Source isn't actually created until an authorized user approves the request.

This chapter tells you how to set up Data Source Maintenance. For more information on how the system works, see **IBM Atlas Suite Users Guide: Data Source Maintenance with IIM** and **IBM Atlas Suite Users Guide: Data Source Maintenance without IIM**.

15.1 Components

The Data Source Maintenance workflow is configured through these Components:

- The Parameters in the **DS_CONFIGURATION** Component set the system-level attributes of the Data Source Maintenance feature.
- Each Parameter in the **DS_APPROVER** Component specifies a Role. A user who's assigned one of these Roles can approve a request to create, update, or deactivate a Data Source. However, the Roles that you list in this Component are *not* automatically granted privileges to view and approve/reject Data Source requests. In addition to adding the Role to this Component, you must give the Role **Map > Read** and **Data Source > Read/Write/Delete** privileges.
- Each Parameter in the **DS_MAPPER** Component specifies a Role. A user who's assigned one of these Roles can create, edit, and deactivate a Data Source through the **Map > Data Sources** module. However, the Roles that you list in this Component are *not* automatically granted privileges to view and approve/reject Data Source requests. In addition to adding the Role to this Component, you must give the Role **Map > Read** and **Data Source > Read/Write/Delete** privileges.
- **DS_NEWCHANGEREASON**, **DS_UPDATECHANGEREASON**, and **DS_DEACTIVATECHANGEREASON** provide options for the Data Source change request menus.

15.2 Data Source Maintenance Profiles

The **Admin > Data Source Maintenance** module controls the fields that are required in order to approve a Data Source change request, and controls the fields that users can see when they're viewing and editing a Data Source. The module's subtabs are:

- **Fields Required for Approval**. This page lists all of the Data Source attributes and lets you mark the ones that are required for approval. To make this mark, hover over the name of the field and then click in the blank (unbordered) checkbox that appears:

- **Default View** lists the fields that are displayed to users (without Data Source Mapper or Approver Roles) who request a new Data Source through the **Local Schedules** or **Matters** modules. To add or remove fields, click the **Select Fields** button and make your selection in the list that appears.
- **Default Edit/Create** lists the fields that are displayed to users (without Data Source Mapper or Approver Roles) who create and edit Data Sources through the **Map** module.
- **Mapper View/Edit/Create** lists the fields that are displayed to users who have a Data Source Mapper Role.
- **Approver View/Edit/Create** lists the fields that are displayed to users who have a Data Source Approver Role.

16 Legal eDiscovery

This chapter tells you how to configure various Legal eDiscovery features.

16.1 Matter Security

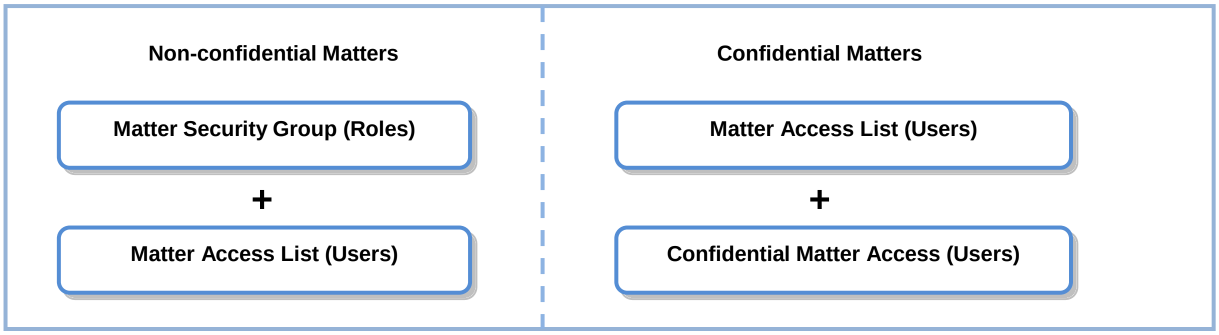
Legal Matters often contain sensitive material. Access to the Matters that are stored in IBM Atlas Suite, therefore, needs to be protected. In addition to (and trumping) the usual Object Permissions (which we'll discuss later), the system provides three methods to define the list of users who have access to a given Matter. In increasing order of protection, the methods are:

- Through the system-wide *Matter Security Groups* (*MSG*). A Matter Security Group comprises a list of Roles. When a new Matter is created, the creator must declare which Security Group the Matter belongs to. All Users who have been assigned the Roles that the declared Security Group comprises will have access to the new Matter. This is the least stringent protection because it only regards Roles. For example, if the **Attorney** Role is added to the **Litigation** Security Group, all Users who have the **Attorney** Role will have access to all Matters that are in the **Litigation** Security Group (unless the Matter is marked as *confidential*—but we'll talk about that in a moment).
- Through a Matter's individual *Access Control List* (*ACL*). This is a list of specific users who need to have access to the Matter, whether or not they're in the MSG. How this list is composed (or, more accurately, *who* gets to compose the list) depends on whether or not the Matter is marked as confidential.
- Through the system-wide *Confidental Matter Access* (*CMA*) list. This is a list of highly-privileged users who are allowed to see Matters that are marked as confidential.

As mentioned in the foregoing, a Matter can be marked as confidential (or not). The actual list of users who have access to a Matter depends on this marking:

- If a Matter isn't confidential, the list of users who have access to the Matter is a combination of the Roles that are defined by the Matter's MSG and the users in the Matter's ACL. The Matter's ACL, for non-confidential Matters, can be modified by anyone in this combined list.
- If a Matter *is* confidential, the list comprises the users in the CMA list and any of the users that they (alone) add to the Matter's ACL. Non-CMA users who are added to the ACL can access the Matter, but they can't modify the ACL—only the CMA users can do that.

Thus, the set of Users who can access a Matter looks like this:



Creating the ACL for a Matter and deciding whether a Matter should be marked as confidential is a per-Matter decision that's made by Legal users.

16.1.1 Confidential Matter Access

IMPORTANT	Make sure you understand the information in the previous section before you perform the operations described here. Depending on how your system is set up, you might only get one chance to define the Confidential Matter Access list.

To modify the Confidential Matter Access list:

1 Go to the **Admin > Confidential Matter Access** module.

2 Click **Add** and then use the **Resource Chooser** to find the users that you want to add.

3 When you've finished, click **Save & Close**.

When the CMA is empty (when the system is first deployed), only the default System Administrator can see (and add users to) the **Confidential Matter Access** module. The users that the System Administrator adds will then be able to see the **Confidential Matter Access module**, but only if they also have **System Administration** or **Organization System Administration** permissions.

IMPORTANT	The System Administrator is *not* added to the CMA list by default. Once the list has been configured, the System Administrator will no longer have access to the list, unless he or she adds him/herself to the list.

16.1.2 Subtleties

There are a few subtleties, here, that need to be understood:

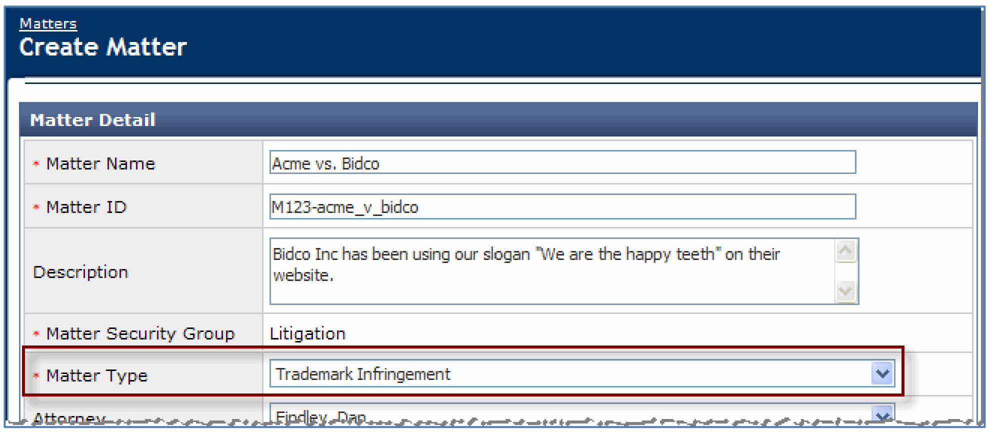
- CMA users aren't automatically added to the ACL for non-confidential Matters. If a user needs to have access to all Matters, confidential or not, you might consider creating a special Role for that user that's added to all Matter Security Groups (in addition to adding the user to the CMA list).
- MSG users can't be selectively removed from a non-confidential Matter. For example: Let's say Jane Doe has a Role that's included in the **Litigation** MSG. A new **Litigation** Matter is created; Ms. Doe will, by definition, have access to

the Matter. Ms. Doe is then added (independently) to the Matter’s ACL, and then, later, removed from the ACL. Despite this later action, Ms. Doe will *still* have access to the Matter because of her **Litigation** MSG Role.

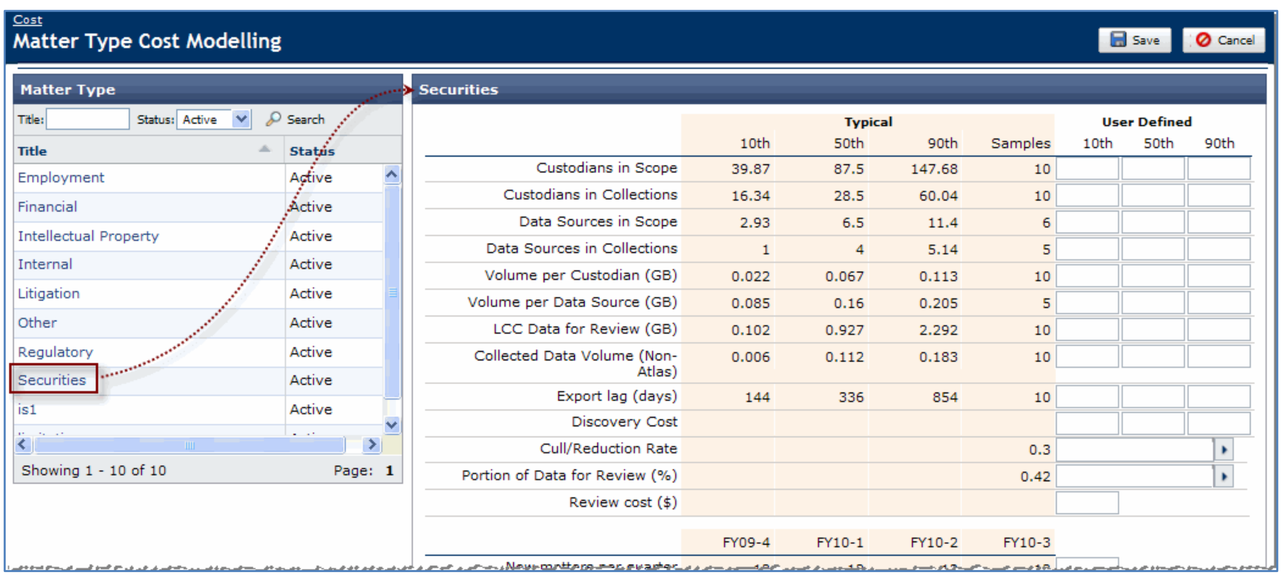
16.2 Matter Types

A Matter’s *Matter Type* identifies its “cost profile”. The eDiscovery Cost Forecasting Management engine gathers statistics for all Matters of the same Type, and uses these statistics when it predicts the cost of an individual Matter of that Type.

Every Matter must be given a Matter Type. The Matter Types that you can choose from when you create a new Matter are displayed in the **Matter Type** dropdown menu on the **Matters > Matter Detail** page:

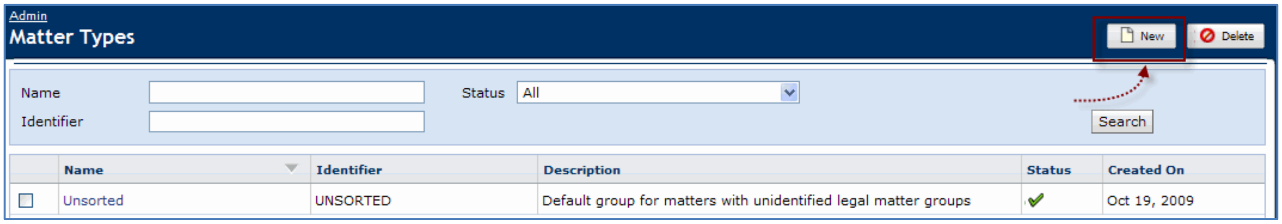


Matter Types also appear throughout the **Costs** module. Here we see the cost profile for the **Securities** Matter Type:

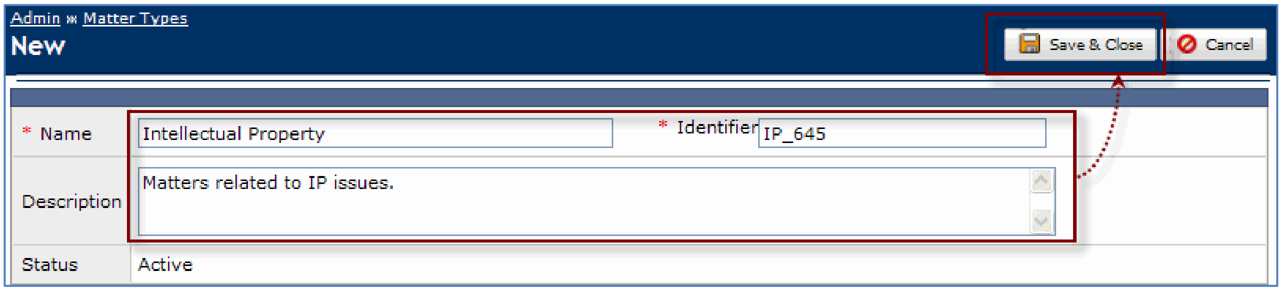


16.2.1 Creating and Deleting Matter Types

Atlas has one built-in Matter Type called **Unsorted**. To create additional Matter Types, go to the **Admin > Matter Types** module and click **New**:

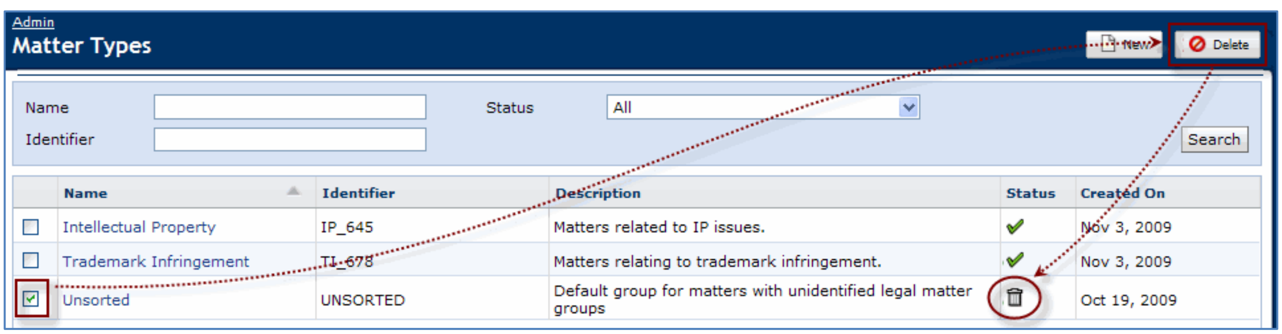


Fill in the fields on the **New** page and click **Save & Close**:



- The **Name** field is the label that's presented to the user in the **Matters** and **Cost** modules and in the eDCF reports. The **Name** should be unique, although be aware that the **Matter Types** module doesn't complain if you specify a name that's already being used.
- **Identifier** is used to identify the Matter Type internally. By identifying Matter Types by **Identifier** rather than by **Name**, you're able to change the name of the Matter Type without dissociating it from the statistics that have already been gathered. The **Identifier** must be unique.
- The **Description** is an optional description of the Matter Type.

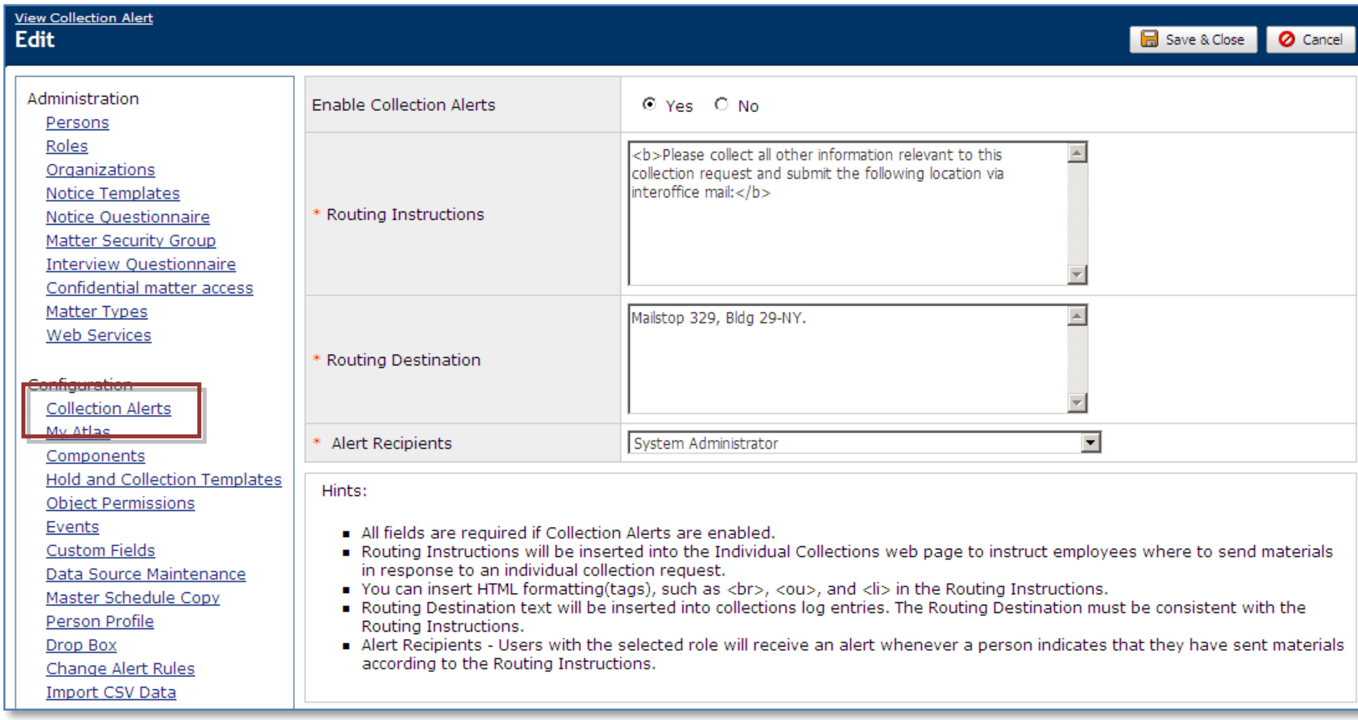
To delete a Matter Type, go to **Admin > Matter Types**, check the Matter Type's checkbox, and click **Delete**:



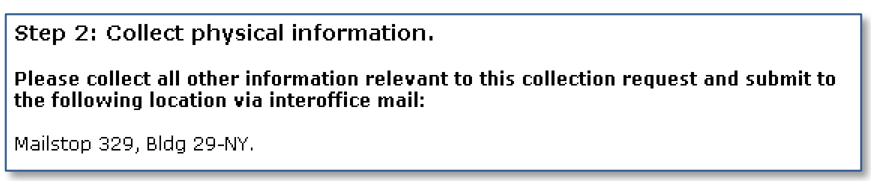
Deleted Matter Types won't appear in the **Matters** or **Cost** modules, but they're not removed from the **Admin > Matter Types** list. Instead, they're set to **Inactive**, as indicated by the trash can icon. By maintaining the list of inactive Matter Types, Atlas makes it less likely for a new Type to unintentionally adopt the statistics that were gathered for a deleted Type (because the old and new Types must have unique **Identifiers**).

16.3 Collection Alerts

When responding to a Collection Notice, a Custodian can indicate that he or she has physical material (hard drives, paper documents, and so on) that needs to be collected. When this happens, the **Collections Routing** Alert is sent to an interested party. The **Admin > Collection Alerts** module lets you enable the Alert and identify its recipients, and define the “collect physical evidence” instructions that are displayed to the Custodian:



The controls in the module are:

Control	Meaning
Enable Collection Alerts	Set this to **Yes** if you want the **Collections Routing** Alert to be sent.
Routing Instructions **Routing Destination**	These two textfields are presented to the Custodian in the **Collect physical information** portion of the Collection Notice: 
Alert Recipients	Use this dropdown menu to specify the Role that will receive the **Collections Routing** Alert. Atlas sends the Alert to all users who are given this Role.

16.4 Drop Boxes

A *Drop Box* is a directory from which files are automatically collected by Atlas. Drop Boxes are typically used by Legal and IT users to collect multiple files at a time, possibly from multiple custodians. See the **IBM Atlas Suite Administrators Guide: Drop Boxes** book for instructions on how to create Drop Boxes for your system.

16.5 Functional Roles

The Components that assign the Functional Roles for Enterprise Discovery Management are:

Component	Function
ATTORNEY	Can be designated as the Attorney in a Matter.
LEGAL ASSISTANT	Can be designated as the Paralegal in a Matter.
LEGAL NOTICE APPROVER	Can approve new or modified Notices and Plans.
INTERVIEWER	Can be designated as the Interviewer in an Interview Log.
COLLECTOR	Can be designated as the Collector in a Collection Log.
TRANSACTION_WORK_ASSIGNOR	Can modify the ownership of a Preservation or Collection Plan.
CONTENT_DISPOSAL_REQUESTER	Can request that a Matter's documents be deleted.
CONTENT_DISPOSAL_APPROVER	Can approve or reject requests to delete a Matter's documents.
CONTENT_DISPOSAL_SUBSCRIBER	Receives Alerts regarding disposal workflow events.
LEGAL_POWER_USER	Can use Hold Notice Templates that are marked as Legal Power User-only and can view the **Who is on Hold** report.
NOTICE_RECIPIENT_REMOVER	Can remove Persons from all Holds and Virtual Interviews.
GLOBAL_HOLD_REMINDER	Can access the **Admin > Global Hold Reminder** module.

In addition, only those users who are designated as **ATTORNEY**s, **LEGAL ASSISTANT**s, **INTERVIEWER**s, or **COLLECTOR**s can have Drop Boxes assigned to them.

16.6 Other Components

There are a number of other Components that control the eDiscovery functionality. Look for the *Legal Matters* chapters in the **IBM Atlas Suite Administrators Guide: Components** book.

17 Notice Templates and User Password Messages

IMPORTANT	In pre-v6 systems, the Templates for a Hold Notice were created in the **Admin > Notice Templates** module (described here). In v6, this is no longer true: Hold Notice Templates are now created through the **Admin > Hold Notice Templates** module. Old (pre-v6) Notice Templates for Holds are *not* migrated to new Hold Notice Templates. If you want to use the old Notice Templates for your new Hold Notices, you have to recreate them in the **Admin > Hold Notice Templates** module.

A *Legal Notice* is a message that notifies users of their obligations with regard to a Legal Hold, Release, Collection, or Virtual Interview. Legal users, typically paralegals, create Legal Notices through the **Matters** module. To standardize your company's Notices (and to make Notice creation easier), you can create a library of *Notice Templates* through the **Admin > Notice Templates** module. A Notice author can select from these Templates as a starting point when creating a new Notice.

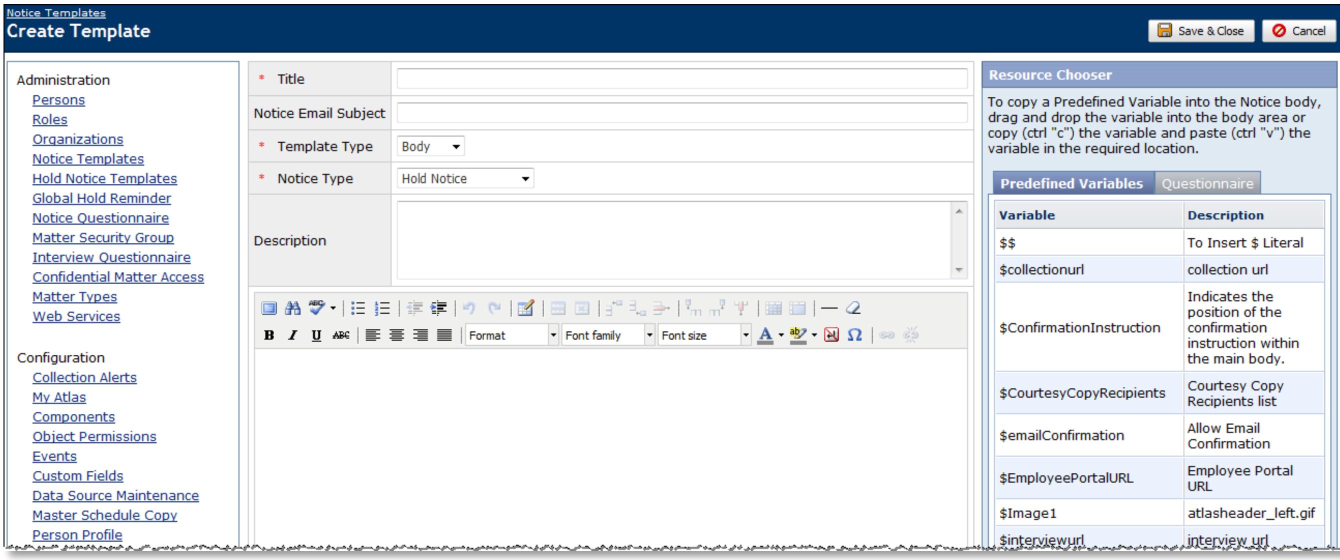
The **Notice Templates** module also lets you create the email messages that are sent to users when they request an initial password and when they request that their current password be reset. This only applies to systems that use Atlas for login authentication.

When creating and working with Notice Templates be aware of the following:

- Legal users don't *have* to use a Notice Template when creating a Notice. They can create Notices from scratch in the **Matters** module (except for Hold Notices, as explained in Hold Notice Templates).
- The exact form of a Legal Notice—the parts that it includes—depends on the type of Notice (Hold, Release, Collection, or Virtual Interview), but they all include four basic parts: an email subject line, and the header, body, and footer of the Notice message itself. The Templates in the Notice Template library contain only these four parts. When the legal user creates an actual Notice, additional information may need to be added to the Template that they select.
- Each Notice Template is designated as the **Header**, **Body**, or **Footer** for a specific type of Notice (the email subject is defined as part of the **Body** Template). For example, if you designate a Template as **Collection/Header**, the Template can only be used as the header in a Collection Notice—it can't be used as the header in a Release or Virtual Interview Notice.
- With regard to Hold Notices, the Notice Templates described here are used for the Notice's "corporate" header and footer, and for the body of the escalate-to-manager message. Templates for the body of the Hold Notice are created through the **Admin > Hold Notice Template** module. See Hold Notice Templates for details.
- In general, if you edit a Template after it has been used to create a Notice, the changes to the Template aren't propagated to that Notice. The exception to this is the (corporate) header and footer for a Hold Notice. For example, if you modify a **Header/Hold** Template that's being used in a Hold Notice that sends Auto-Reminders, all Reminders that are sent after that point will use the new version of the Template.
- When you delete a Notice Template, the Template is completely erased from the system—it isn't merely deactivated.

17.1 Creating a Notice Template

To create a Legal Notice Template, go to the **Admin > Notice Templates** module and click **New**. This brings up the **Create Template** page:



The attributes and tools on the page are:

Attribute	Meaning
Title	This is the name of the Template as it will appear to the legal user who's constructing a Notice. The name must be unique.
Notice Email Subject	The subject line that will appear in the Notice email. This only applies to **Body** Templates.
Template Type **Notice Type**	These two menus let you designate how and where a Notice author can use the Template. • The **Template Types** are **Header**, **Body**, and **Footer**. • The **Notice Types** are **Hold**, **Release**, **Individual Collection**, **Interview**, **Obtain Password**, and **Reset Password**. The combinations of **Template** and **Notice Type**s are explained in Template and Notice Types.
Description	An optional description. The description is only displayed in the Notice Templates module; it isn't shown to the legal user who's using the Template.
Editor	You use the editor to compose the content of the Template. You can include text formatting and images.

<table>
<tr><th>Attribute</th><th colspan="2">Meaning</th></tr>
<tr><td rowspan="3">Resource Chooser</td><td colspan="2">When you compose the text of the Notice Template, you can include the Predefined Variables that are presented in the Resource Chooser on the right. These are placeholders that represent the recipient’s name, the name of the Attorney for the Matter, a link to the web form that lets users upload documents, and so on. For a description of these placeholders, including an explanation of which placeholders can be used in which type of Notice, see <u>IBM Atlas Suite Users Guide: Legal Notice Placeholders</u>.</td></tr>
<tr><td>IMPORTANT</td><td>You must not use the Hold confirmation placeholders ($confirmationInstructions, $emailConfirmation, $NoticeResponseURL, and so on) in the Notice Templates.</td></tr>
<tr><td>IMPORTANT</td><td>Ignore the Questionnaires tab. Questionnaires only apply to the bodies of Hold Notices, which are created through the Hold Notice Templates module.</td></tr>
</table>

17.2 Template Types and Notice Types

The way a Notice Template can be used, by a Notice author, depends on its **Template Type** and **Notice Type** designations. The combinations of these types are described in the following sections.

17.2.1 Notice Type: Hold

17.2.1.1 Header and Footer

Depending on the issuance type (as explained in Hold Notice Templates), a Hold Notice can contain as many as three headers. The **Header** and **Footer** Templates that you create here define a Hold Notice’s “corporate” header and footer. These are intended to be used as boilerplates that bracket the rest of the content in the Hold Notices: The corporate header appears at the beginning of the Notice (before all other headers and the body) and the footer appears at the end. The corporate header and footer appear in the Hold Notice email that’s sent to the custodian, and in the representation of the Notice in the custodian’s **My Holds** tab.

Keep in mind that if you modify a Notice Template that’s used as a Hold Notice’s corporate header or footer, all subsequent issuances of that Hold Notice will use the modified versions.

17.2.1.2 Body

The combination of **Notice Type: Hold** and **Template Type: Body** creates the body of the escalation message that can be sent to a custodian’s manager if the custodian doesn’t confirm the hold within a designated amount of time. The escalation message body can only be created through a **Hold/Body** Notice Template—the Notice author can’t create the message body while creating the Hold Notice.

17.2.2 Notice Type: Release and Individual Collection

The Notice for a Release or Collection is simple: It contains an email message line, and, in the content of the message, a header, body, and footer. All of these parts can be created through the **Notice Templates** module.

17.2.3 Notice Type: Interview

An Interview Notice comprises two parts: The email message that announces the Interview (the "message content"), and the Interview Questionnaire web form that holds the Interview questions themselves (the "interview content").

- The **Header** and **Footer Template Types** pertain to the interview content; they bracket the questions that make up the interview as it appears in the web form. The header and footer don't appear in the email message.
- The **Body Template Type** creates the body of the email message; it doesn't appear in the Interview web form.

17.2.4 Notice Type: Obtain Password and Reset Password

These two Notice Types aren't Notices in the legal sense; they're simply email messages that are sent to a user when the user requests, through buttons on the Atlas login page, an initial password or a password reset. This only applies to systems that use Atlas for login authentication.

If you're using Atlas for authentication and want to take advantage of the password messages, you should create a *single* set of header/body/footer Templates for **Obtain Password**, and another (single) set for **Reset Password**. The three parts are stitched together to create a unified obtain or reset password email message.

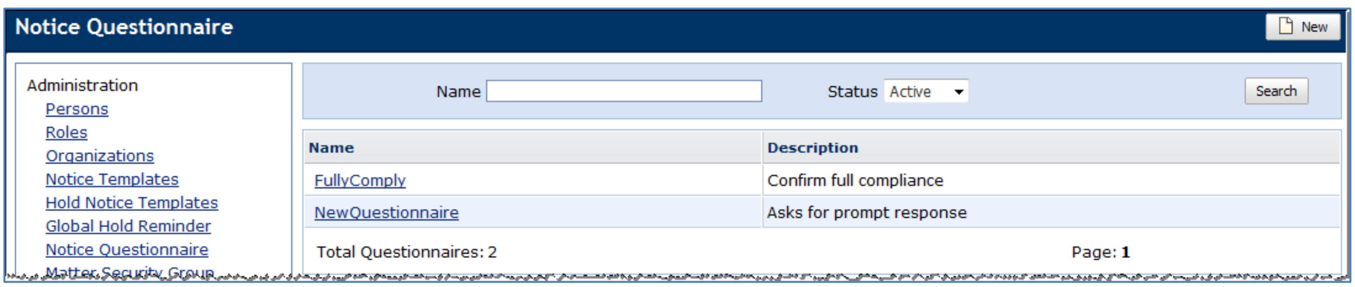
18 Notice Questionnaires

A *Notice Questionnaire* is a list of questions that can be inserted into the body of a Hold Notice to capture the fact that a person has received, read, and acknowledged the Notice. You can also add a Notice Questionnaire to a Hold Notice Template (which we'll look at in the next chapter).

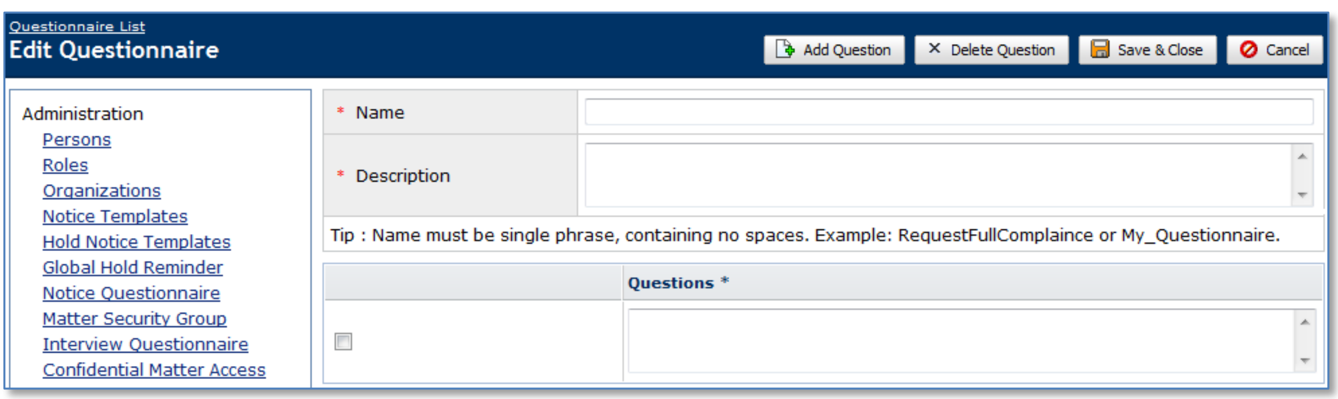
IMPORTANT	Notice Questionnaires don't apply to Collection or Virtual Interviews Notices.

18.1 Creating a Notice Questionnaire

The Notice Questionnaires that are defined in your system are listed in the **Admin > Notice Questionnaire** module:

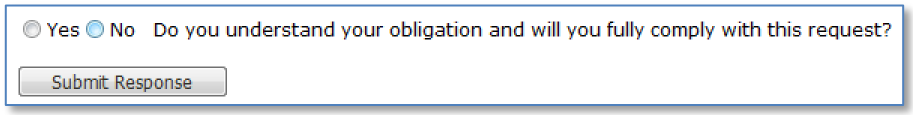


To create a Notice Questionnaire, click **New**. This brings up the E**dit Questionnaire** page:



The attributes on the page are:

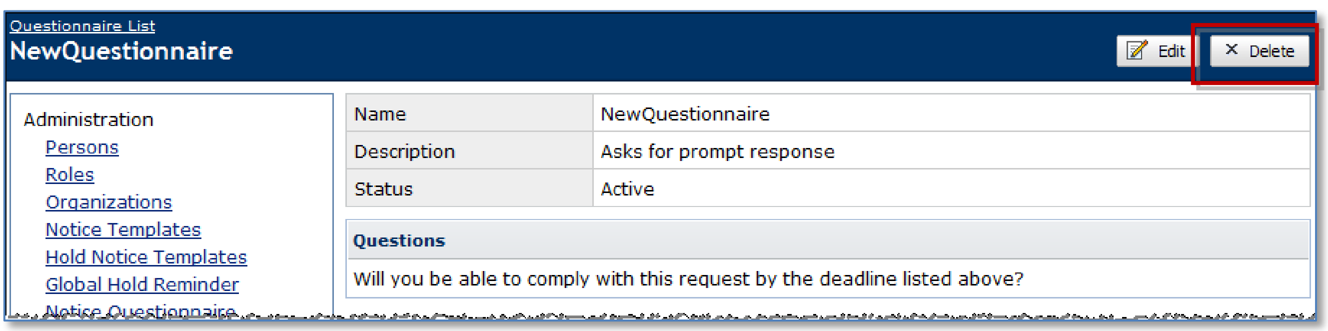
Attribute	Meaning
Name	This is the name of the Questionnaire. Questionnaire names must be unique and may not contain spaces. When the Questionnaire is presented for use to the Hold Notice (or Hold Notice Template) author, the "**$Q:**" prefix is added to the name—you don't add these characters yourself.
Description	A description of the Questionnaire. The description is only displayed here—it isn't shown to the Notice author.

Attribute	Meaning
Questions	This is a list of the questions that make up the Questionnaire. Each question must have a yes-or-no answer. You only supply the question, here; you don't supply the answer. When the question is displayed to the Notice recipient, a **Yes/No** radio button is automatically added. For example:  To add additional questions, click the **Add Question** button at the top of the page. To delete a question, check its checkbox and click **Delete Question**.

After you've finished composing the Questionnaire, click **Save & Close**.

18.2 Deleting a Notice Questionnaire

To delete (deactivate) a Questionnaire, click its name in the main Questionnaire list, and then click **Delete** on the Questionnaire's details page:



This doesn't remove the Questionnaire from the system, it simply marks it as inactive. Questionnaire names must be unique across *all* Questionnaires, including those that are inactive.

18.3 Notes

- Notice Questionnaires must be pre-defined—that is, they can only be created through **Notice Questionnaire** module. Unlike with Virtual Interview Questionnaires, the Notice author isn't able to create Notice Questionnaires.
- In order for a Questionnaire to be regarded as confirmed, the Notice recipient must answer **Yes** to all questions.
- A single Notice Questionnaire, **FullyComply**, is provided by default. The text of the question is: *Do you understand your obligation and will you fully comply with this request?* This Questionnaire can't be deleted and you can't change its name.
- Hold Notices are sent as email messages and are added to the recipient's **My Holds** list. Some email systems, however, don't display the Questionnaire controls properly. If you want to exclude the Questionnaire from the email message, set the **INCLUDE_QUESTIONNAIRE_IN_EMAIL** Parameter in the **WEB_NOTICE_RESPONSE_MANDATORY** Component to **False**; by default, it's set to **True**

19 Hold Notice Templates

IMPORTANT	In pre-v6 systems, the Templates for a Hold Notice were created in the **Admin > Notice Templates** module. In v6, this is no longer true: Hold Notice Templates are now created through the **Admin > Hold Notice Templates** module (described here). Old (pre-v6) Notice Templates for Holds are *not* migrated to new Hold Notice Templates. If you want to use the old Notice Templates for your new Hold Notices, you have to recreate them in the **Admin > Hold Notice Templates** module.

The **Admin > Hold Notice Templates** module lets you create templates that legal users can use to create the Hold Notices that they construct. There are two types of Hold Notice Templates:

- The *Content Template* contains the body of the Notice message, and includes a “Corporate” header and footer.
- The *Rules Template* contains additional message text (email subject, Notice-specific header) and defines how the Notice is processed: Its due date, whether it needs to be approved and confirmed, the Confirmation Instructions, the Escalation Rules for non-confirmation, and so on. The parameters in the Rules Template can be locked so that a Notice author can’t modify them.

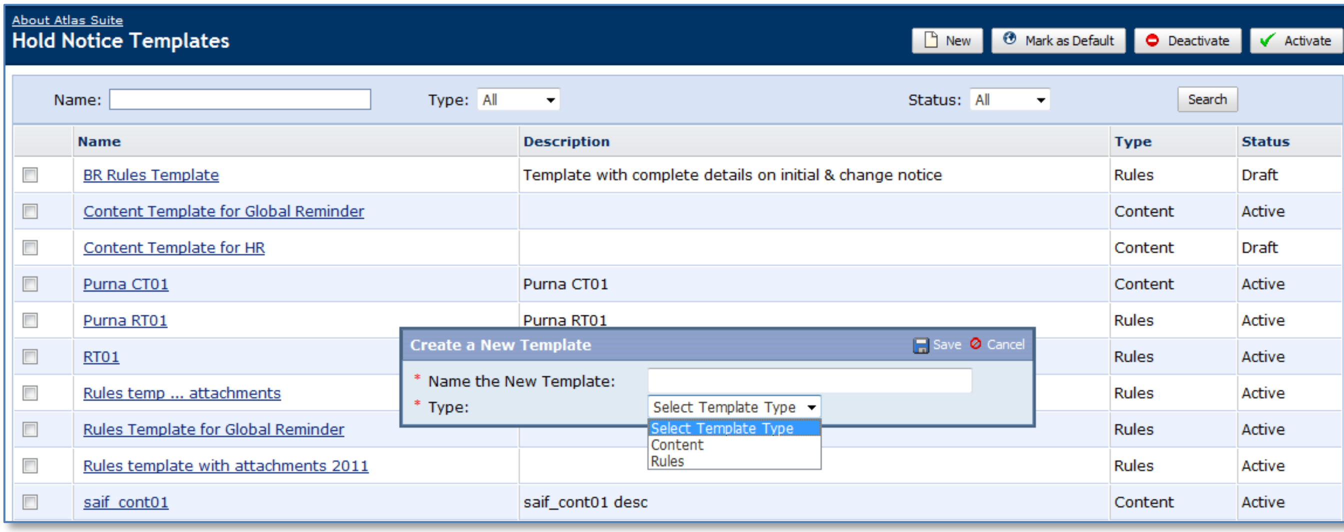
When creating a new Hold Notice, the legal user must select one Content Template and one Rules Template.

As a Hold Notice Template author, you can’t force a pairing of Content and Rules Templates—Hold Notice authors can mix-and-match Templates as they wish. You can, however, suggest an affinity between a Content and a Rules Template through careful naming (“Content for Hold with VI”/”Rules for Hold with VI” for example).

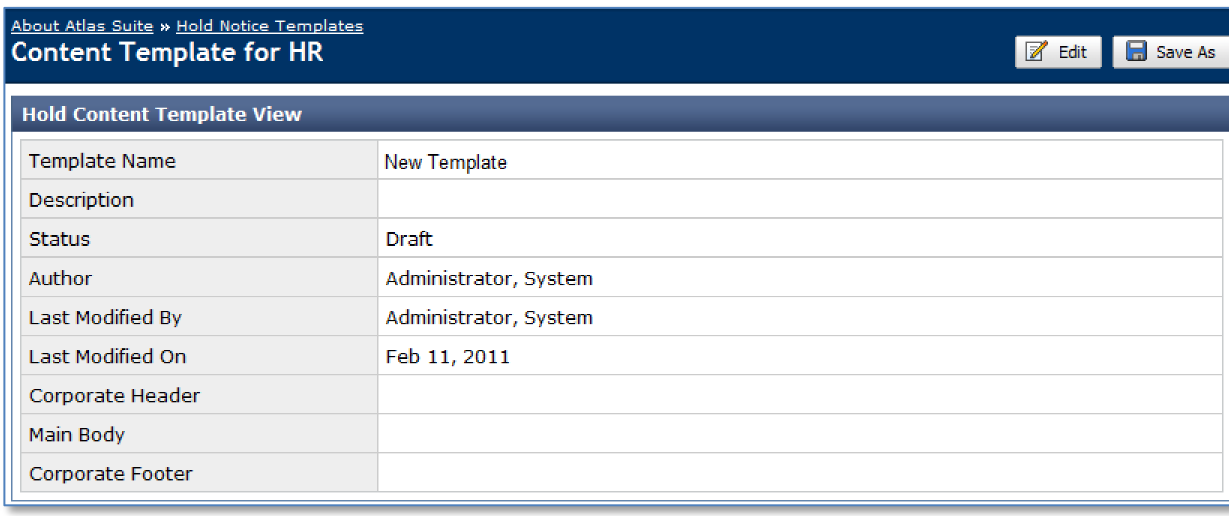
19.1 The Content Template

The Content Template contains the main body of the Notice. Notably, the Template *doesn’t* include Confirmation Instructions, which are created through a Rules Template.

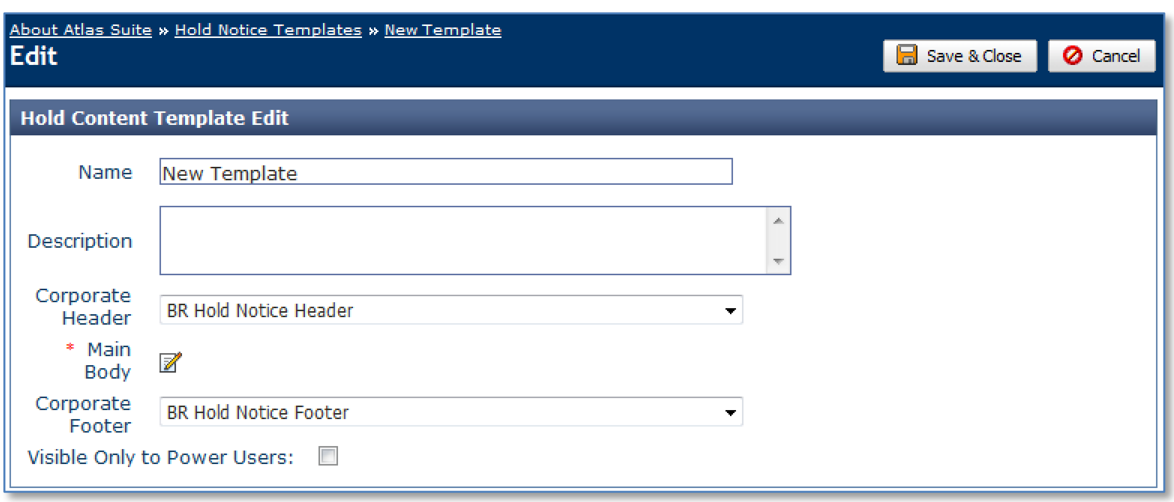
To create a Content Template, go to **Admin > Hold Notice Templates**, click **New**, select **Content** from the **Type** menu, give the Template a name, which must be unique across all Content Templates, and click **Save**:



The **Hold Content Template View** page is displayed:



To finish the definition of the Template, click **Edit**; this opens the Template Editor:



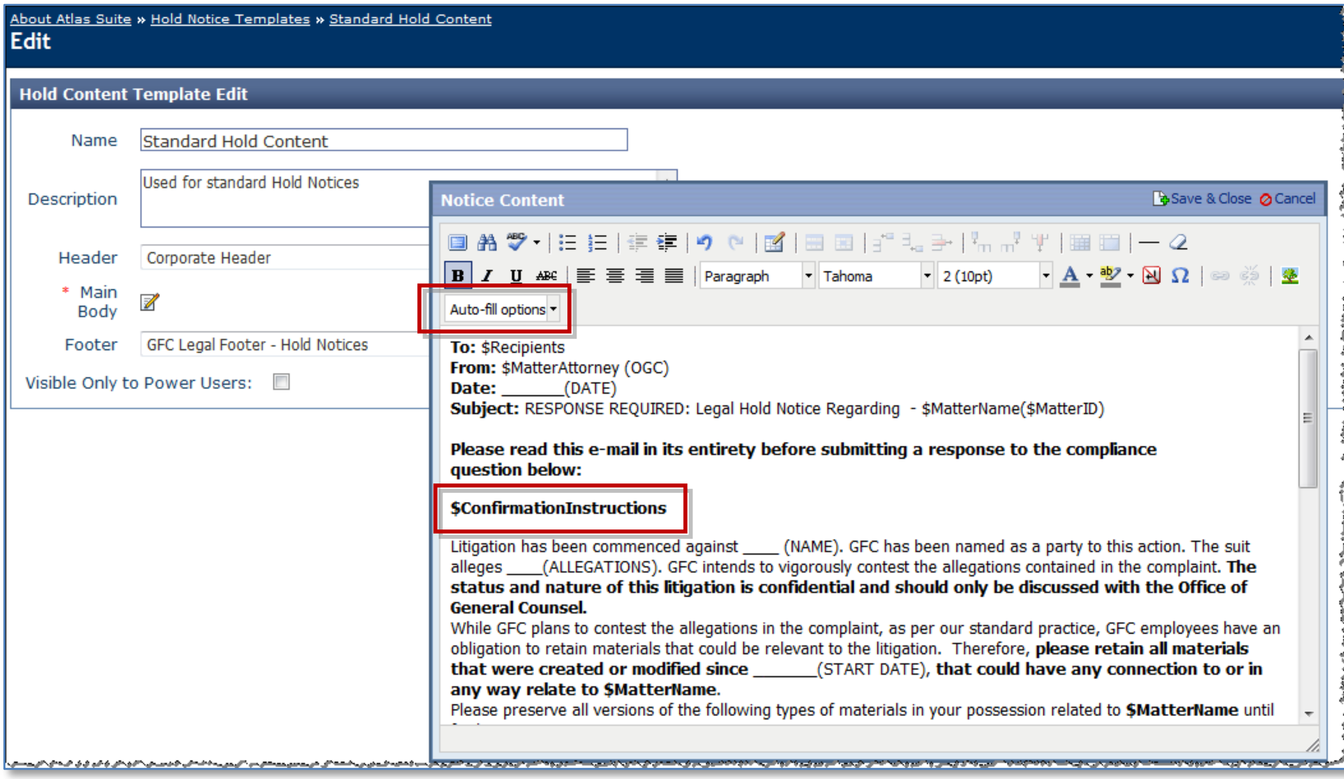
The fields are:

Control	Meaning
Name	This is the name that you gave the Template. All Template names must be unique within their type.
Description	An optional description. The description is only displayed in the Hold Notice Templates module; it isn't shown to the legal user who's creating a Hold Notice.
Corporate Header	A *Corporate Header* is an optional, corporate boilerplate header for all Hold Notices. The **Corporate Header** menu is populated with the **Header/Hold** Templates that you created through the **Admin > Notice Template** module. An additional Notice-specific header is included as part of the Rules Template.
Main Body	Contains the text of the main part of the Notice. To view and edit the text, click the edit icon ( ). We'll look at the Main Body in more detail in the next section.
Corporate Footer	This is like **Corporate Header**, but is populated with the **Footer/Hold** Templates.
Visible Only to Power Users	If you check this checkbox, only *Legal Power Users* will be able to use this Template when creating a Hold Notice. This feature is provided as a way to protect sensitive Templates from general use.The Legal Power Users are defined through the **LEGAL_POWER_USER** Component.

When you're finished defining the Content Template, click **Save & Close**.

19.1.1 Content Main Body

The Main Body editor lets you define the body of the Notice message. It includes a drop down menu (**Auto-fill options**) that lists the placeholders that you can use in the body. Of particular importance is the **$ConfirmationInstructions** placeholder, which represents the Confirmation Instructions that are defined in the Rules Template.

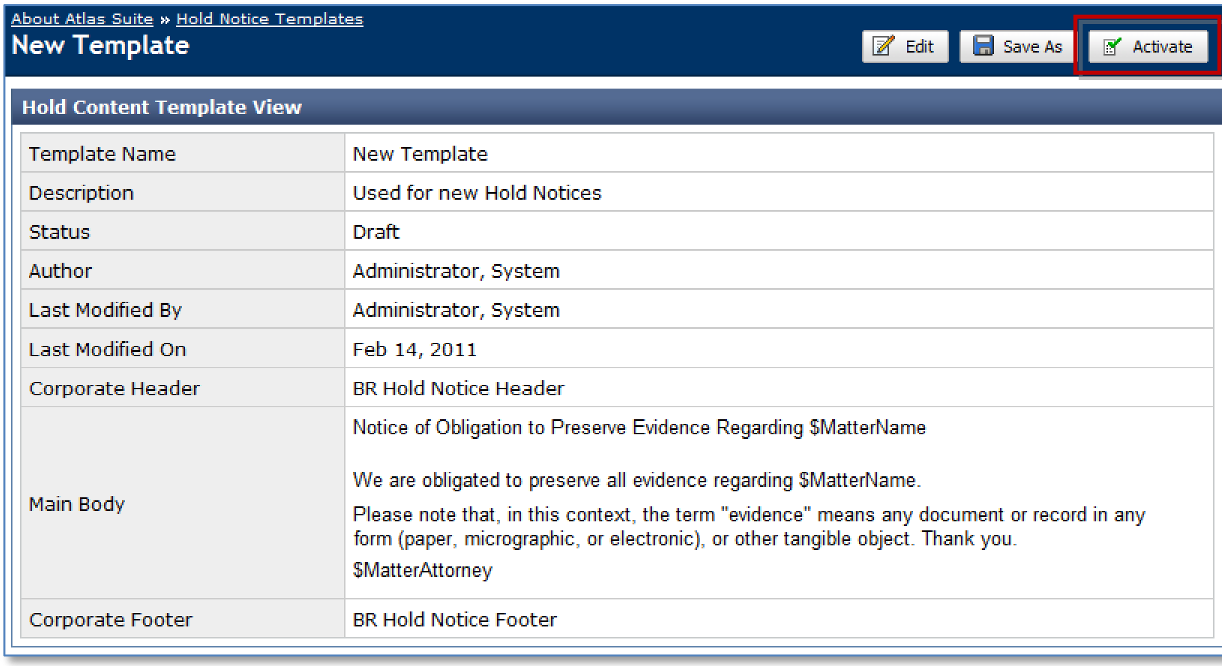


If a Hold Notice requires confirmation, **$ConfirmationInstructions** must be added to the body of the (actual) Notice. If you don't include the placeholder in the Content Template, the Notice author can add it later, when composing the actual Hold Notice.

Unlike the elements in the Rules Template, which we'll look at later, you can't lock the Main Body in the Content Template.

19.1.2 Activating and Cloning

Back in the **Hold Content Template View** page, you'll see an **Activate** button added to the top of the page:


About Atlas Suite » Hold Notice Templates

New Template

Edit | Save As | Activate

Hold Content Template View

Template Name	New Template
Description	Used for new Hold Notices
Status	Draft
Author	Administrator, System
Last Modified By	Administrator, System
Last Modified On	Feb 14, 2011
Corporate Header	BR Hold Notice Header
Main Body	Notice of Obligation to Preserve Evidence Regarding $MatterName We are obligated to preserve all evidence regarding $MatterName. Please note that, in this context, the term "evidence" means any document or record in any form (paper, micrographic, or electronic), or other tangible object. Thank you. $MatterAttorney
Corporate Footer	BR Hold Notice Footer

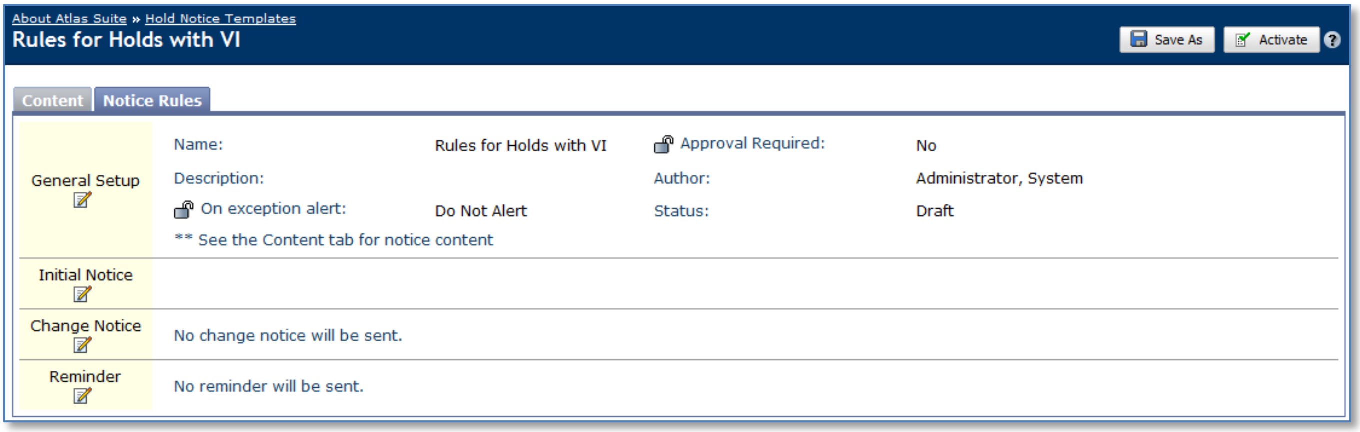
A freshly created Hold Notice Template is in **Draft** state; draft Templates aren't displayed to Notice authors. In order to make a Template usable, you must activate it. You can also activate Templates from the main **Hold Notice Templates** page.

The **Save As** button lets you make a clone of the Notice Template. When you click **Save As**, you're asked to supply a new name, and then are taken to the **Hold Content Template View** page for the new Template.

19.2 Rules Templates

A Rules Template defines the rules for how a Notice is processed. It contains *almost* everything about the Notice that isn't defined in the Content Template. There are a few attributes, such as the list of designated Approvers (for Notice's that need approval), that are defined in the actual Hold Notice.

To create a new Rules Template you click **New** on the main **Hold Notice Templates** page, give the Template a unique name, select **Rules** from the **Type** menu, and click **Save**. The page that appears looks like this:



The page comes up with the **Rules** tab selected; this is where you'll do most of your work. The **Content** tab is provided so you can see how the Notice will look when a Rules Template is combined with a Content Template.

The Rules are divided into four sections:

- The first section, **General Setup**, gives the name and description of the Template (not the Notice itself), how to handle exceptions, and so on.

The other three sections correspond to a type of Notice issuance:

- The **Initial Notice** section defines the "rules" for the first issuance of the Notice. This includes the email subject line, a message header, whether the Notice needs to be confirmed, escalation rules if a recipient doesn't respond, and so on.
- The rules in the **Change Notice** section are used when an Initial Notice is modified and reissued. This gives the Notice author a chance to explain to recipients who have already received the original Notice that this "next generation" Notice replaces the previous issuance.
- The **Auto-Reminder** section provides rules for regularly recurring Notices.

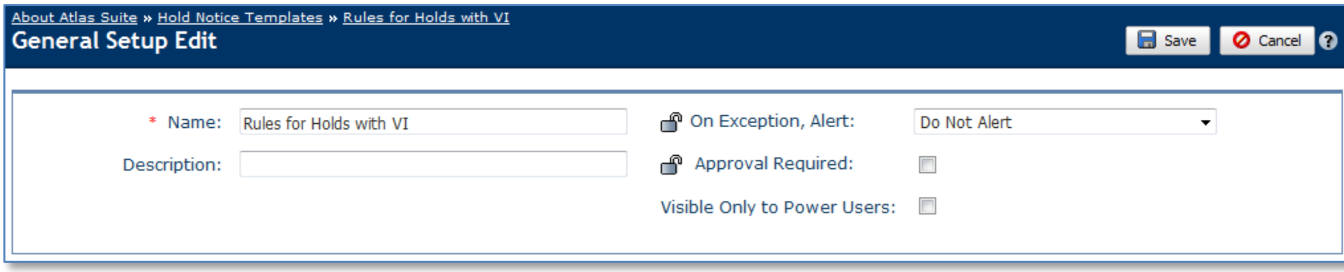
To edit a section, click the corresponding edit icon ( ).

NOTE Throughout the Rules Template, the lock icons (and) are controls that let you declare whether a Notice author can or can't modify the value of a parameter that's set in the Template.

The Notice Rules page contains **Save As** and **Activate** buttons; these buttons behave the same was as they do for Content Templates.

19.2.1 General Setup

When you edit the **General Setup** section, you see this:

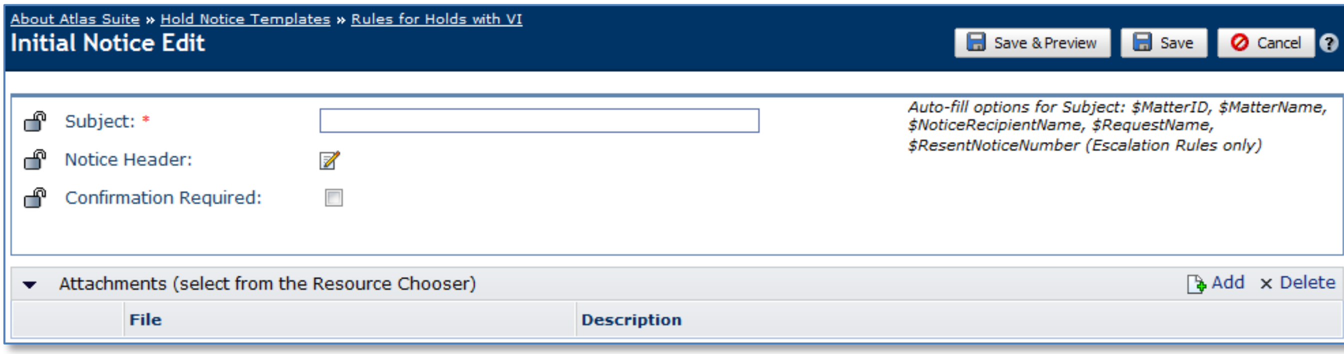


The fields are:

Control	Meaning
Name	This is the name that you gave the Template. All Template names must be unique within their type.
Description	An optional description. The description is only displayed in the Hold Notice Templates module; it isn't shown to the legal user who's creating a Hold Notice.
On Exception, Alert	The menu lets you select the recipient(s) of the Alerts that are generated if a Notice is undeliverable, if a recipient can't comply with the Hold, or if a recipient doesn't respond in the alloted amount of time. The **Attorney** and **Paralegal** selections send the Alerts to everyone on the Attorney Alerts and Paralegal Alerts lists for the Matter, respectively. **All** sends the Alerts to both lists.
Approval Required	If you check this checkbox, the Notice must be approved before it can be published. Note that the Template doesn't let you specify the Approvers—that's the job of the Notice author. As with the **On Exception, Alert** attribute, you can lock your choice.
Visible Only to Power Users	If you check this checkbox, only *Legal Power Users* will be able to use this Template when creating a Hold Notice. This feature is provided as a way to protect sensitive Templates from general use.The Legal Power Users are defined through the **LEGAL_POWER_USER** Component.

19.2.2 Initial Notice

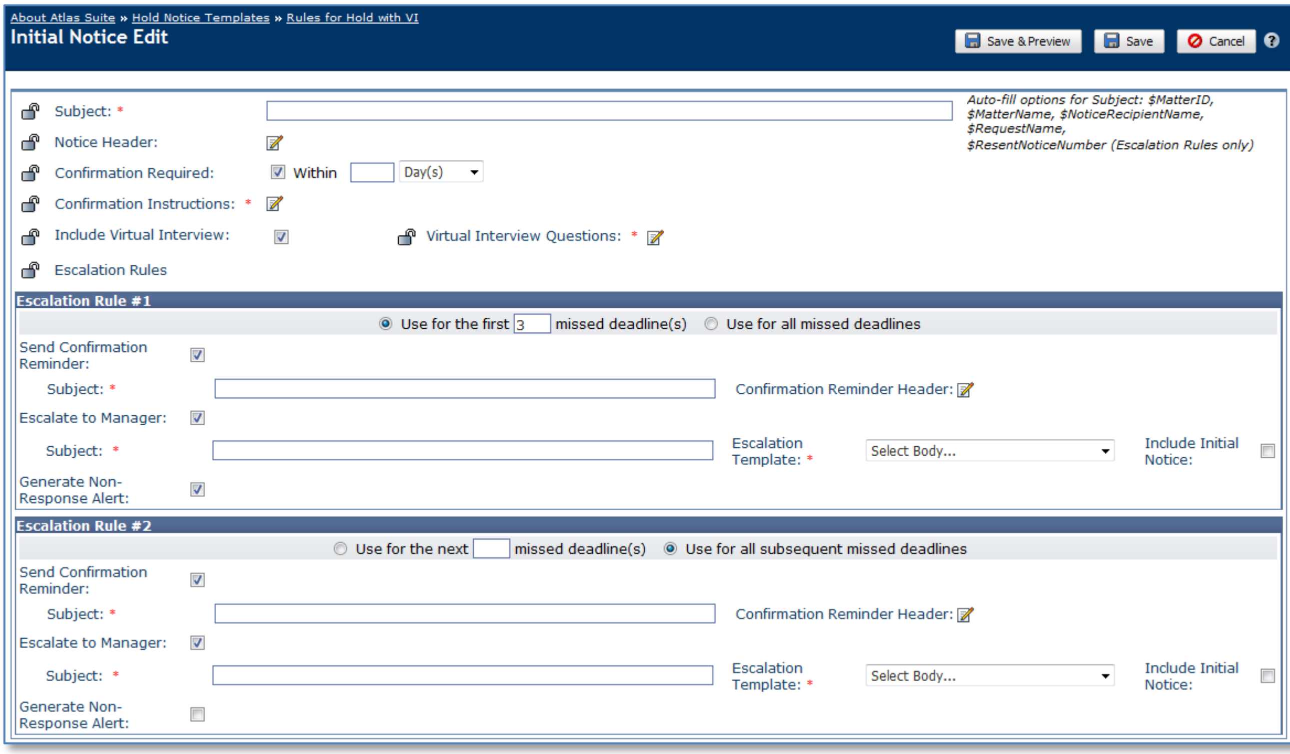
The Initial Notice section lets you set up the Rules for the initial issuance of the Notice.



Control	Meaning
Subject	The subject line in the Notice email message. The instructions at the right list the placeholders that you can use in the **Subject** text. You have to copy-and-paste or type the placeholders into the **Subject** text field. Again, see the **IBM Atlas Suite Users Guide: Legal Placeholders** for an explanation of the placeholders.
Notice Header	This is an additional header that's placed after (below) the Corporate Header that's defined in the Content Template. To view and edit the text, click the edit icon ( ). The editor includes a drop down menu (**Auto-fill options**) that lists the placeholders that you can use in the header. Unlike the Corporate Header, this header isn't selected from the Notice Templates list.
Confirmation Required	If you check this checkbox, recipients are required to confirm that they can or can't comply with the Hold. It also adds controls to the UI, which we'll look at later, that let you set the confirmation deadline and the Escalation Rules for non-confirmation.
Attachments	Lets you add files to the Notice.

19.2.2.1 Confirmation Required

When the **Confirmation Required** checkbox is checked, additional controls are displayed:



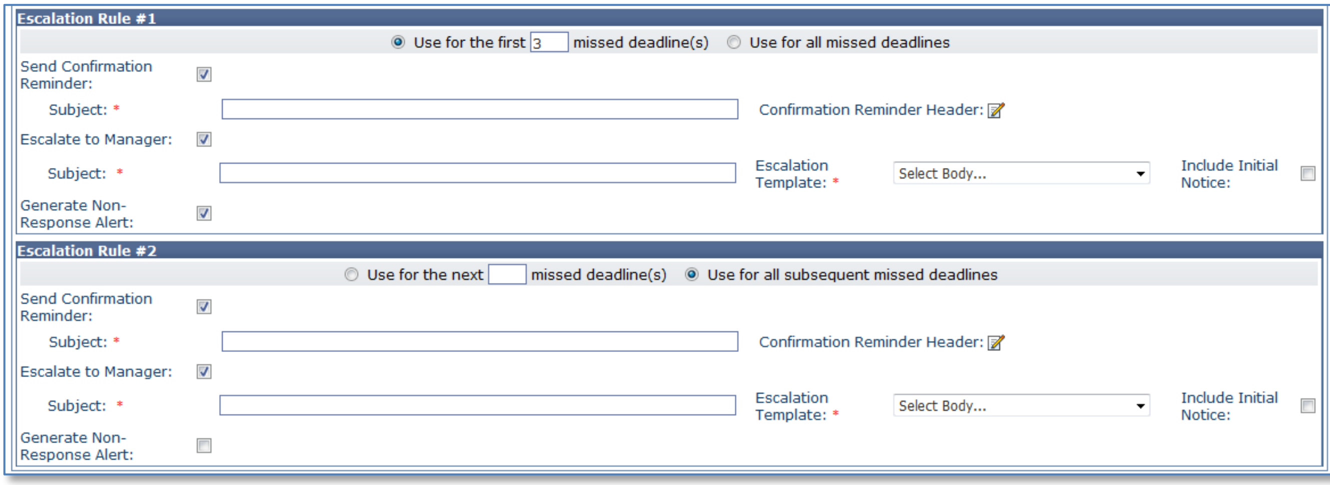
Control	Meaning
Within	The **Within** field lets you set the deadline for the recipient's confirmation. If a recipient misses the deadline, the first escalation rule (**Escalation Rule #1**) is triggered. The **Within** value is also used to set the frequency of subsequent escalations. For example, if you set the value to **3 Days**, a non-responsive recipient will cause escalation actions every three days.
Confirmation Instructions	Click the edit icon to open an editor that lets you create the Confirmation Instructions that are sent to the Notice recipients. Unless the legal team wants to record the confirmations themselves, the instructions should include one of the confirmation placeholders or a Notice Questionnaire. The placeholders and Questionnaires that are available for use in the instructions are presented in separate drop down menus.
Include Virtual Interview	If you want to use a Virtual Interview as the confirmation method, check the **Include Virtual Interview** checkbox (it's unchecked by default). The **Virtual Interview Questions** editor appears. When you click the edit icon you're presented with a list of the Virtual Interview Questionnaires that have been added to your system. You can only add one Questionnaire, you can't modify the contents of the Questionnaire, and you can't add stand-alone questions. The Notice author, on the other hand, can do all of these things (as long as the Questionnaire setting isn't locked). If you're using a Virtual Interview, you must add either **$interviewurl** or **$interviewurlview** to the Confirmation Instructions.
Virtual Interview Questions	
Escalation Rules	Lets you lock the configuration of the escalation rules, which we'll look at next.

19.2.2.2 Escalation Rules

When confirmation is required, you can create a series of *Escalation Rules*. These are actions that are taken when a Notice recipient doesn't respond within a given amount of time.

The Escalation Rules can be defined as a set of stages: If a recipient fails to respond within the first *N* deadlines (where a deadline is a recurring event with a frequency that's set to the **within** value described in the previous section), **Escalation Rule #1** is used (once for each missed deadline). If the recipient fails to respond for the next *M* deadlines after that, **Escalation Rule #2** is used, and so on. In a typical setup, each successive rule is harsher than the last.

By default, two stages are displayed. If we fully-expanded rule #1, we see this:



<table>
<tr><th>Control</th><th>Meaning</th></tr>
<tr><td>Use for the first/next deadline(s)</td><td rowspan="2">These radio buttons let you set the longevity of the rule. If you select Use for the first/next deadline(s), the rule is triggered only a certain number of times, after which the escalation moves to the next rule. Use for all [subsequent] missed deadlines means the rule will continue to be triggered .

When you set a rule to Use for the first/next..., another rule panel is added so you can create the next rule.

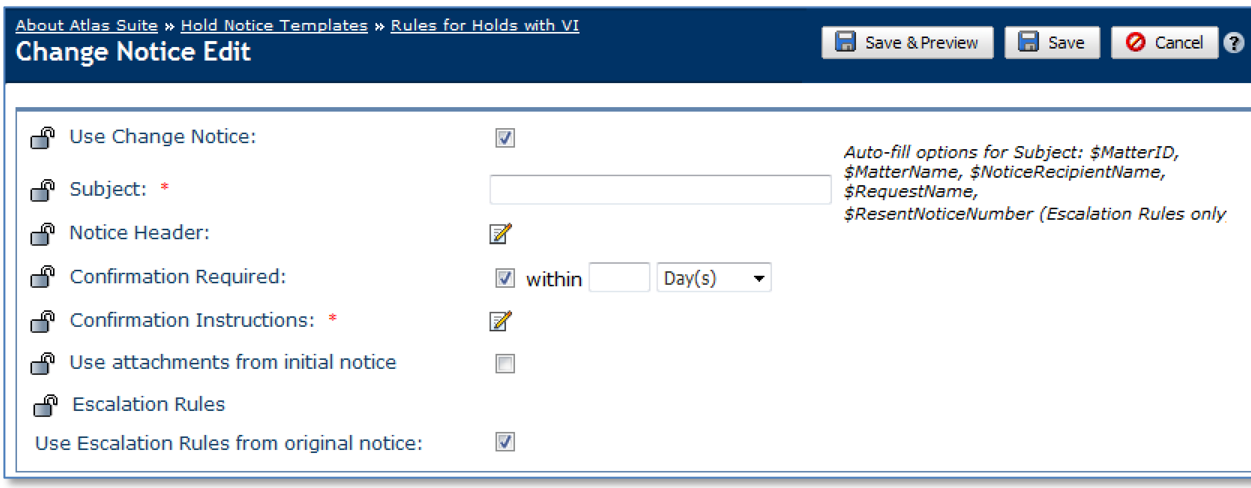
If you only want to trigger N escalations and then stop, set a Use for the first/next… value in the first rule, and then select Use for all subsequent missed deadlines for the second rule but leave the rule empty, as shown above</td></tr>
<tr><td>Use for all [subsequent] missed deadlines</td></tr>
<tr><td>Send Confirmation Reminder</td><td rowspan="3">If you want to resend the Initial Notice to recipients who haven't responded in time, check Send Confirmation Reminder. You then must provide a Subject line for the email that will be sent, and you can (optionally) supply a Confirmation Reminder Header that's placed between the Corporate Header and the Initial Notice Header. The Confirmation Reminder Header editor lets you add a selected set of placeholders.</td></tr>
<tr><td>Subject</td></tr>
<tr><td>Confirmation Reminder Header</td></tr>
<tr><td>Escalate to Manager</td><td rowspan="4">Causes an email message to be sent to the unresponsive recipient's manager. You must supply a Subject for the email, and select a Notice Template from the Escalation Template menu. Include Initial Notice lets you add the text of the Initial Notice to the email.</td></tr>
<tr><td>Subject</td></tr>
<tr><td>Escalation Template</td></tr>
<tr><td>Include Initial Notice</td></tr>
</table>

Control	Meaning
Generate Non-Response Alert	If you want the **Notice Non-Response** Alert to be generated as part of the escalation, check this checkbox. The Alert is sent to the **On Exception, Alert** selection in the **General Setup** section.

19.2.3 Change Notice

After a Notice has been published, it becomes read-only and the **Modify Content** button is added to the Notice UI. It's through this button that the Notice author can create a new version of the Notice that takes the place of the original issuance (which is deactivated).

In some cases, a Notice author may want to supply a slightly different email subject line or Notice header that explains to the recipients who received the original issuance that this new Notice takes the place of the old one. To support this, the Rules Template has a **Change Notice** section that overrides the processing rules that are defined in the **Initial Notice** section:



Control	Meaning
Use Change Notice	If you want to use the Change Notice feature, check this checkbox. If you leave it unchecked, the processing rules from the Initial Notice are used when a Notice is modified. The rest of the controls on the **Change Notice Edit** page aren't displayed if **Use Change Notice** is unchecked.
Subject	The subject line in the Change Notice email message. The instructions at the right list the placeholders that you can use in the **Subject** text. You have to copy-and-paste or type the placeholders into the **Subject** text field.
Notice Header	An optional header that, if supplied, replaces the Initial Header. If you don't supply a **Notice Header** value, the Change Notice uses the Initial Header.
Confirmation Required…Within	These fields behave in the same was as the confirmation settings for the Initial Notice. The only difference is that if confirmation is required and you don't supply Confirmation Instructions here, the instructions from the Initial Notice are automatically used (they're copied into the Confirmation Instructions editor).
Confirmation Instructions	

Control	Meaning
Use Attachments from Initial Notice	If checked, any files that were attached to the Initial Notice are attached to the Change Notice.
Escalation Rules	These fields let you set (and optionally lock) the Escalation Rules for the Change Notice. If you uncheck **Use Escalation Rules from Initial Notice**, the UI in which you create Escalation Rules are added to the panel, as explained in the Initial Notice section.
Use Escalation Rules from Initial Notice	

19.2.4 Auto-Reminder

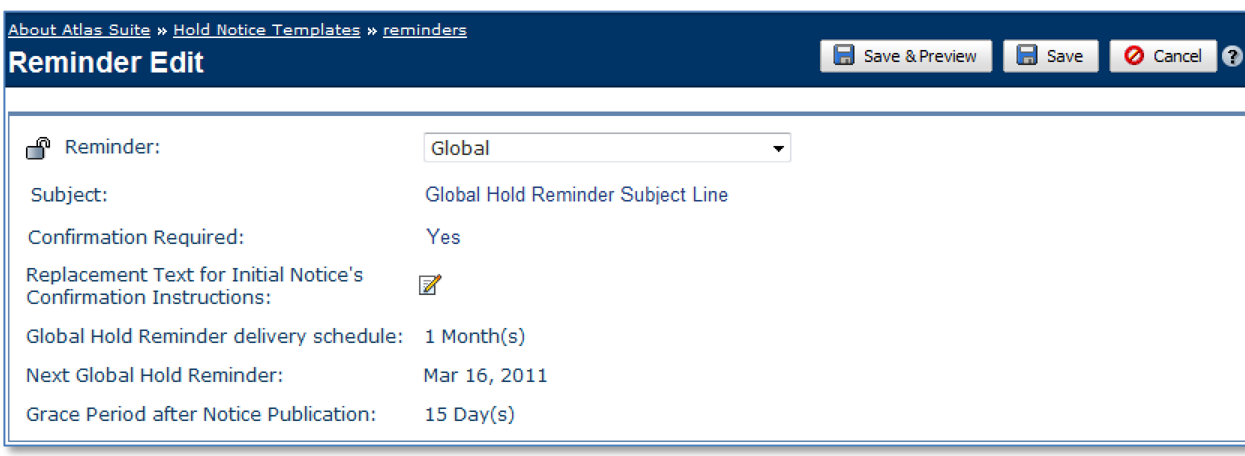
A Notice can be regularly reissued as a series of *Auto-Reminders* that tell the recipients that they must make sure they're still in compliance with the Hold. The **Auto-Reminder** section lets you create the processing rules for these reminders.

When you edit the **Auto-Reminder** section, you're presented with an **Auto-Reminder** menu that lets you select the type of reminder:

- **None** means no Auto-Reminders will be sent. If you choose **None**, none of the other controls are displayed.
- **Global** uses the Global Hold Reminder, as described in the Global Hold Reminder chapter.
- **Notice-specific** lets you create an Auto-Reminder that's specific to this Template.

19.2.4.1 Using the Global Hold Reminder

If you select **Global** from the Reminder menu, you see the Global Hold Reminder's attributes as they're defined through the **Admin > Global Hold Reminder** module:



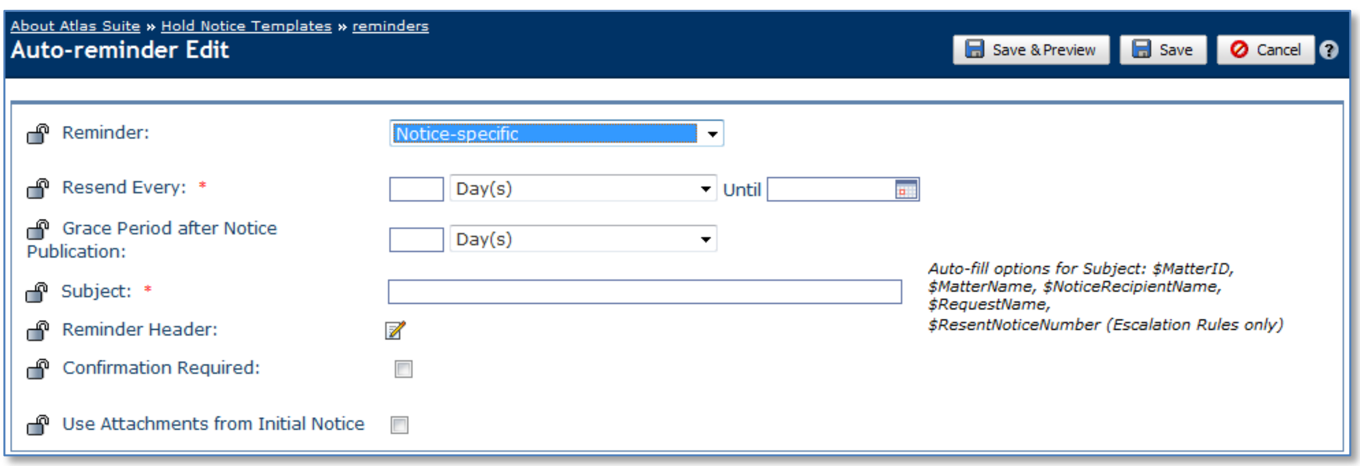
The one attribute that isn't defined by the Global Hold Notice—and the only attribute that's editable—is the **Replacement Text…** field:

Control	Meaning
Replacement Text for Initial Notice's Confirmation Instructions:	This editor lets you compose a message that will replace the Confirmation Instructions that were added to the Initial Notice. This text is used in the Notice as it's displayed in the **My Holds** module. Keep in mind that the Notices that are listed in the tab can't be confirmed individually, so the Confirmation Instructions are ineffective. If you leave this field blank, the original Confirmation Instructions are (simply) removed from the Reminder.
	IMPORTANT The **Replacement Text…** control is displayed only if the **GLOBAL_HOLD_REMINDER > USE_FOR_CONFIRMATION** Component Parameter is set to **Yes**.

See the Global Hold Reminder chapter for an explanation of the other attributes, and for more information about the Global Hold Reminder in general.

19.2.4.2 Using Notice-Specific Reminders

The notice-specific Auto-Reminder editor looks like this:



Control	Meaning
Resend Every…Until	Sets the frequency with which the Auto-Reminder will be sent, and the date upon which it will stop being sent.
Grace Period	This is the amount of time after the original Hold Notice issuance during which a Custodian is exempt from the Auto-Reminder. For example, let's say the next Auto-Reminder for the "Acme vs Acme" Hold Notice is scheduled to be sent on May 10th, the frequency is 15 days, and the **Grace Period** for the Auto-Reminder is 5 days. If John Smith is added as recipient between May 5th and May 10th, he won't be sent the May 10th Auto-Reminder; his first Auto-Reminder will be sent on May 25th.

Control	Meaning
Subject	The subject line in the Auto-Reminder email message. The instructions at the right list the placeholders that you can use in the **Subject** text. You have to copy-and-paste or type the placeholders into the **Subject** text field.
Reminder Header	An optional header for the Reminder. The header replaces the header that was added to the Initial Notice.

The rest of the controls are the same as those in the Change Notice.

19.3 Previewing the Notice

After you've created a Content Template and Rules Template, you can preview the Notice that the combination of the two Templates will create by going to a Rules Template and clicking the **Contents** tab. The page lets you select a Content Template (through the **Select a content template…** menu), and shows you how the different versions of a Notice that's based on the two Templates will appear to the Custodians (although, of course, many of the placeholders will be shown in their "***$variable***" form since they can't be replaced with real values).

The **Select message to preview** menu lets you choose the version of the Notice (**Initial Notice**, Conf**irmation Reminder N for Initial Notice**, **Change Notice**, **Confirmation Reminder N for Change Notice**, and so on) that you want to see. If you use the Global Hold Reminder in your Rules Template, the menu will include the **Global Reminder in My Holds** item, which shows you how the Notice will look as it's listed in the **My Holds** module.

The parts of the Notice that are defined in the Rules Template (but not the Content Template) are editable, just as they are in the **Rules** tab.

19.4 The Template List and the Default Templates

The Templates that have been defined for your system are listed on the main **Admin > Hold Notice Templates** page. There can be two versions of the same Template: One that's **Active** and another in **Draft** form. When you edit a Template, a draft version is created. When the draft is activated, it replaces the original Template.

You can designate one Content Template and one Rules Template to act as the defaults for their types. The default Templates are selected by default in the Template menus that are presented to Notice authors. To mark a Template as the default, select it in the list and click the **Mark as Default** button.

20 Global Hold Reminder

A Hold can be configured such that an *Auto-Reminder Notice* is issued periodically to remind Custodians of their legal obligations, with a separate Auto-Reminder email message for each Hold. If a Custodian is involved in dozens or hundreds of Holds, the volume of Auto-Reminder email can be inundating; confirming each Hold one-by-one (when confirmation is required) can be tedious.

Instead of the separate-Auto-Reminder-per-Hold approach, you can configure your Notices to use the *Global Hold Reminder* email message that summarizes the Custodian's obligations across all Holds (or a subset), and that includes a link to the **My Holds** page in Atlas where the Custodian can confirm all of the Holds with a single mouse click (if the Global Hold Reminder is configured to use this feature).

There's a single Global Hold Reminder configuration for the entire system. The Reminder can be applied selectively to Hold Notice Templates and to individual Hold Notices themselves—not all Notices need to use the Global Hold Reminder feature. On the **My Holds** page, the Notices that can be confirmed through the Global Hold Reminder are listed in the **Global Reminder** tab (they're also listed, although without confirmation methods, in the **Current Notices** tab).

IMPORTANT	Notices that are grouped under the **Global Reminder** tab can't be confirmed one-by-one. They can only be confirmed as a group through the **Confirm** button.

In addition, the Global Hold Reminder includes a *Global Reminder Report*. This Report lists and describes the Custodians to whom the Reminder has been sent.

20.1 The GLOBAL_HOLD_REMINDER Component

The Parameters in the **GLOBAL_HOLD_REMINDER** Component provide system-wide configuration of the Global Hold Reminder. The Parameters are described in the **IBM Atlas Suite Administrators Guide: Components** book; briefly, they are:

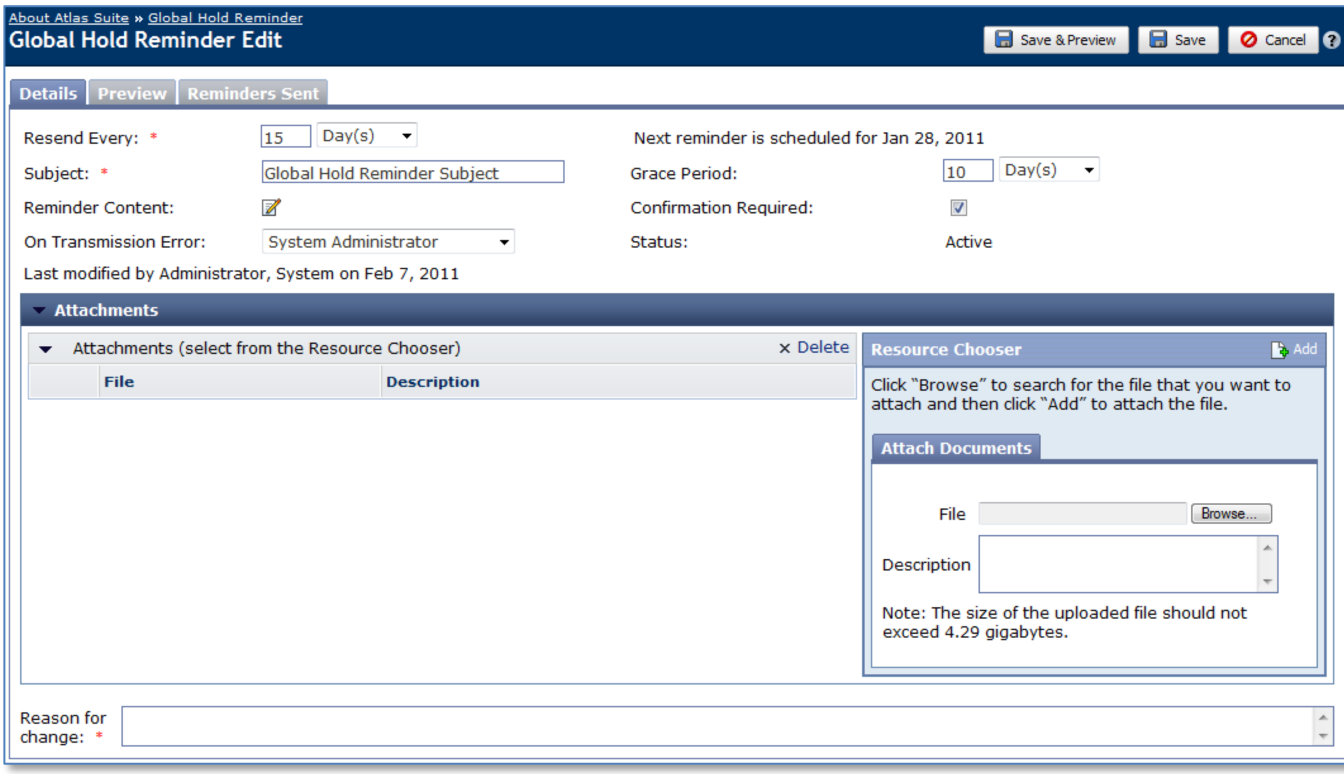
- The most important parameters are **NOTIFICATION_ONLY** and **USE_FOR_CONFIRMATION**. The values of these two Parametesr determine how the Global Hold Reminder will be used with regard to the confirmation settings in the Notices it controls.
- **CONFIG_ROLE** takes a single Atlas Role as a value. Users who have this Role are allowed to edit the Reminder, but they can't view the Reminder Report.
- **REPORT_ROLE** is also a single Atlas Role. Users who have this Role can't edit the Reminder, but they can generate and view the Reminder Report.

IMPORTANT	Users who have these Roles must also have System Administrator or Organization System Administrator permissions

IMPORTANT	When generated from the **Global Hold Reminder** module, the **Recipient Report** bypasses the Matters' Access Control Lists. Thus, it's possible for administrators to view information for Matters that they don't otherwise have access to.

20.2 Configuration

To configure the Global Hold Reminder, go to the **Details** tab of **Admin > Global Hold Reminder** and click **Edit**. The **Global Hold Reminder Edit** page appears:



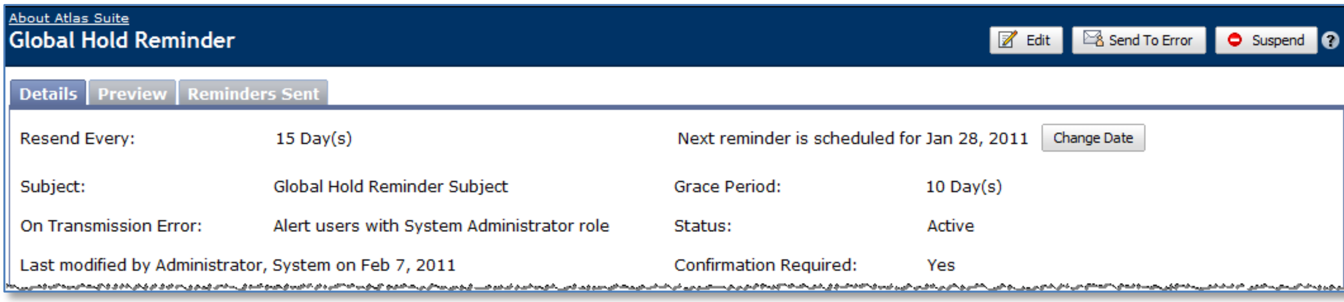
The editable controls are:

Control	Meaning
Resend Every	This sets the frequency with which the Reminder is sent, starting from the time the Reminder configuration is saved.
Subject	The subject line in the Reminder email.
Reminder Content	Click the edit icon ( ) to edit the body of the Reminder email. The message editor provides a subset of the Notice placeholder variables: • **$$** inserts a $ symbol. • **$EmployeePortalURL** is a link to the Custodian's **My Holds** page. • **$NoticeRecipientName** is the name of the Custodian. • **$Image1** is the `Properties/ibm_logo_w_3.gif` image file. By default, this is the IBM logo.

Control	Meaning
On Transmission Error	This is an Atlas Role to whom a **Global Hold Reminder Bounce** Alert is sent if the Reminder couldn't be delivered to one or more of the Custodians.
Grace Period	This is the amount of time after the original Hold Notice issuance during which a Custodian is exempt from the Reminder. For example, if the next Global Hold Reminder is scheduled to be sent on May 10 and the **Grace Period** is 5 days, any Custodians that are added to a Hold Notice (including new Hold Notices) on or after May 5^{th} won't be sent the May 10^{th} Reminder (assuming that the Notice uses the Global Hold Reminder feature).
Confirmation Required	**IMPORTANT** This checkbox is displayed only if **GLOBAL_HOLD_REMINDER > NOTIFICATION_ONLY** is **No** and **GLOBAL_HOLD_REMINDER > USE_FOR_CONFIRMATION** is **Yes**. If checked, the Notices that are controlled by the Global Hold Reminder require confirmation. In this case, the **Confirm** button is added to the **Global Reminder** tab in the **My Holds** module, thus allowing Custodians to confirm all of the Holds that are listed on the page. If it's unchecked, the Notices don't require confirmation. In this case, the **Confirm** button isn't added to the **Global Reminder** tab. In both cases, the Notices are listed (in identical form) in both the **Current Notices** and **Global Reminder** tabs, and the confirmation instructions from their Initial Notice issuances (if any) are replaced with text that's defined in the **Auto-Reminder** section of the Hold Notice. **IMPORTANT** If the **Confirmation Required** checkbox appears at all, then the confirmation requirement in the Global Hold Reminder overrides (at the time that the Global Hold Reminder message is sent) the requirement defined by the Initial Notice. For example, if an Initial Notice requires confirmation but the Global Hold Reminder doesn't, a custodian is expected to confirm the Initial Notice, but is relieved of the obligation to confirm once he or she receives the Global Hold Reminder.
Attachments	The **Attachments** section lets you add files that will be sent with the Reminder.
Reason for Change	You must always provide a description of why you're editing the Reminder.

After you've finished, click **Save** (or **Save & Preview**, which takes you to the **Preview** tab).

Back in the main **Details** view, you'll see a summary of the configuration, and some additional controls:



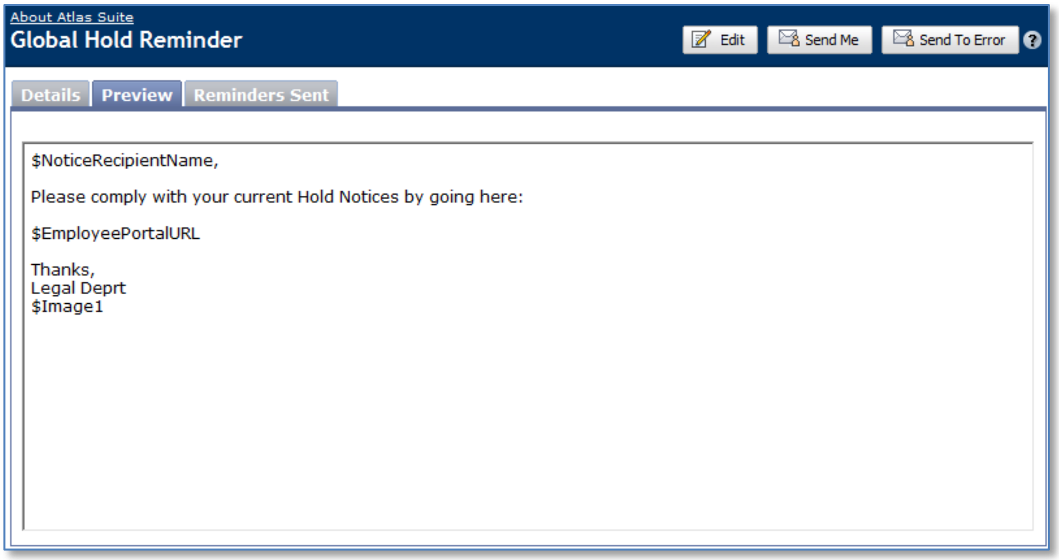
The additional controls are:

Control	Meaning
Edit	Takes you to the Reminder editor.
Send to Error	This tells the system to schedule a retransmission of the Global Hold Reminder that will be sent, the next time the **Send Reminder** Timer Task runs, to those recipients who didn't receive a previous issuance of the Reminder because of a transmission error (SMTP server failure, faulty email address, and so on). Resending doesn't affect the scheduling of the next Reminder issuance. **IMPORTANT** The **Send to Error** action doesn't cause the Global Hold Reminder to be immediately sent. It only schedules the transmission.
Supend/Resume	These buttons let you suspend and resume transmission of the Reminder. When you resume transmission of a suspended Reminder, the next issuance date is recalculated based on today's date. For example, if you suspend a Reminder whose next issuance date is July 1st and then resume it on June 30th, the next issuance will be reset to July 30th.
Change Date	This button pops open a calendar that lets you manually set the date of the next Reminder issuance. Subsequent Reminders are reckoned from the date you set. You can't change the date while the Reminder is suspended.

The bottom part of the page (not shown) lists the Reminder's attachments and provides a history of changes (including suspensions and resumptions).

20.3 Previewing

The **Preview** tab shows the Reminder email message as it will appear to the recipients. Note that the placeholders aren't expanded:

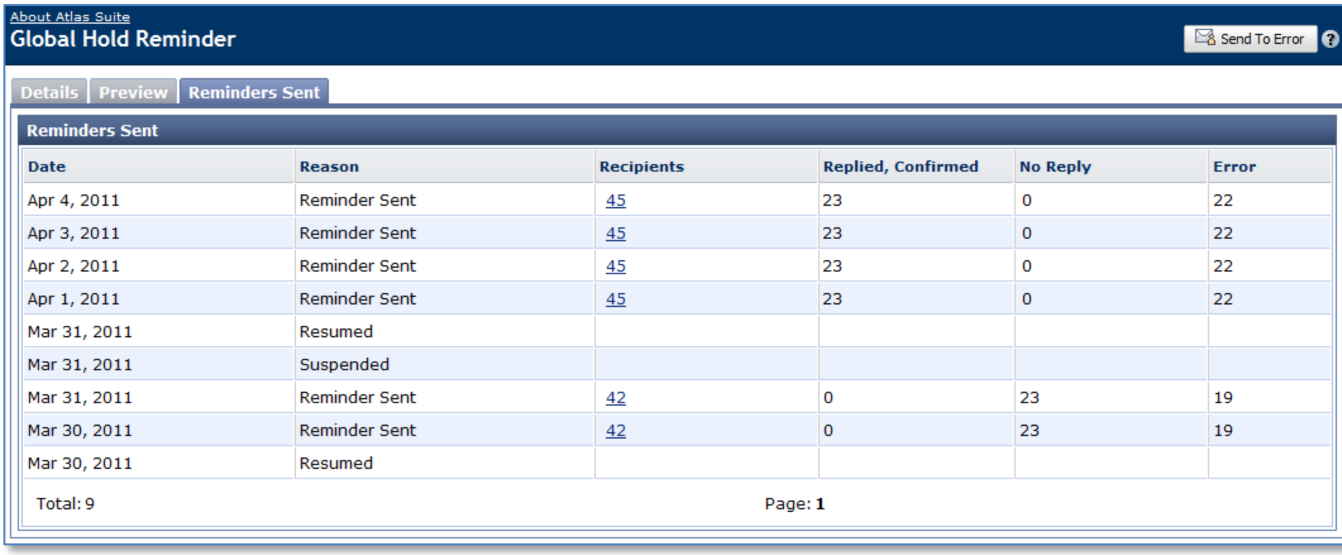


The buttons at the top of the page let you…

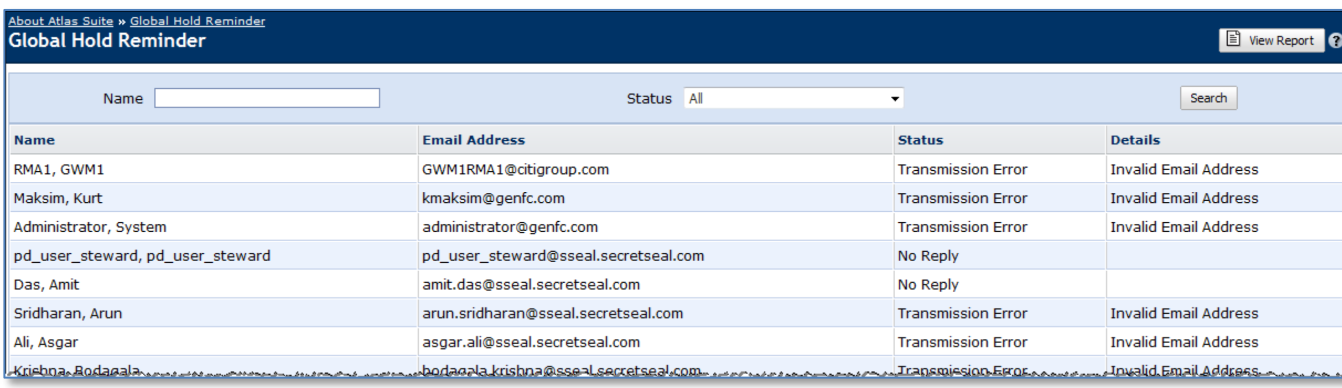
- **Edit** the content (this is the same as the **Reminder Content** editor described above).
- Send a copy to yourself (**Send Me**).
- **Send to Error** is the same as on the **Details** page: It schedules a retransmission of the Global Hold Reminder that's sent to recipients who are in **Transmission Error** status.

20.4 Reminders Sent

The **Reminders Sent** tab is a list of Global Hold Reminder issuances, including the reason the Reminder was sent, and the number of recipients and their responses:



When you click a link in the **Recipients** column, you're taken to a list of the Custodians who received that specific issuance of the Reminder:

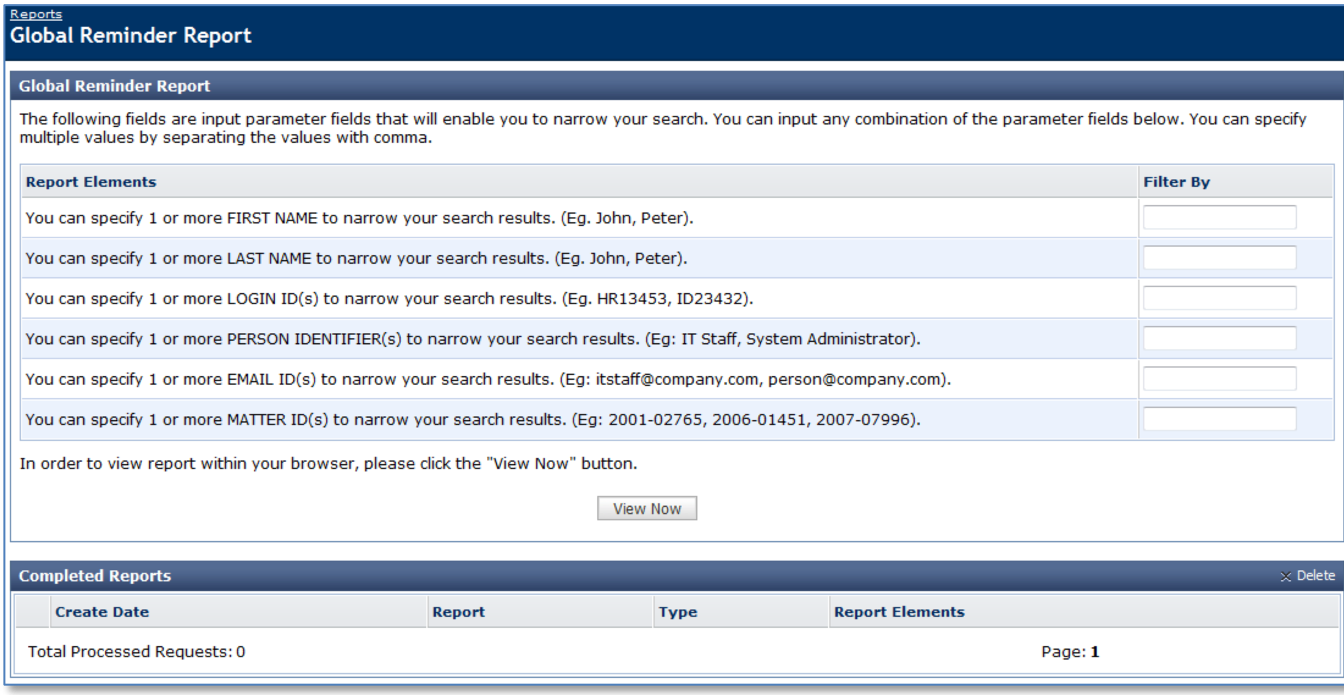


You can filter the list based on Custodian name and status (**No Reply**, "**Replied, Confirmed**", **Transmission Error**, **All**). The **Details** column is only filled in if the status is **Transmission Error**.

20.5 The Global Reminder Report

The **Global Reminder Report** is similar to the recipients list described above, but it provides more detailed information.

You get to the report by clicking **View Report** on the recipient's list. This takes you to a page that lets you filter the recipient list:



The Report lists the recipients you've selected, and then provides sublists of each of the original Notices that caused them to receive the Reminder.

NOTE As mentioned earlier, in order to see the Report you must have the Role identified by the **GLOBAL_HOLD_REMINDER > REPORT_ROLE** Parameter.

IMPORTANT The **Global Reminder Report** is only available through the **Admin > Global Hold Reminder** module. It can't be added to the **Reports** tab or the **Personal Favorites** tray in **My Atlas**.

20.6 Applying the Global Hold Reminder

You can apply the Global Hold Reminder to a Hold Notice Template and to individual Hold Notices.

To apply the Reminder to a Hold Notice Template, do this:

1. Go to **Admin > Hold Notice Templates** and select a Rules Template (or create a new one).
2. Click the Edit icon in the **Reminder** section.
3. Select **Global** from the **Reminder** menu.
4. If the Global Hold Reminder is being used for confirmation (as declared through the **GLOBAL_HOLD_REMINDER > USE_FOR_CONFIRMATION** Component Parameter), you can supply text that will replace the confirmation

instructions that were sent in the Initial Notice. The replacement instructions will be displayed on the Custodian's **My Holds** page. To create replacement instructions, click the **Replacement text…** edit icon.

For more information, see the Hold Notice Templates chapter.

The process for applying the Global Hold Reminder to an individual Hold Notice is similar to that for Hold Notice Templates, but performed, of course, through the **Matters** module. For more information, see the **Legal Hold Notices** Users Guide.

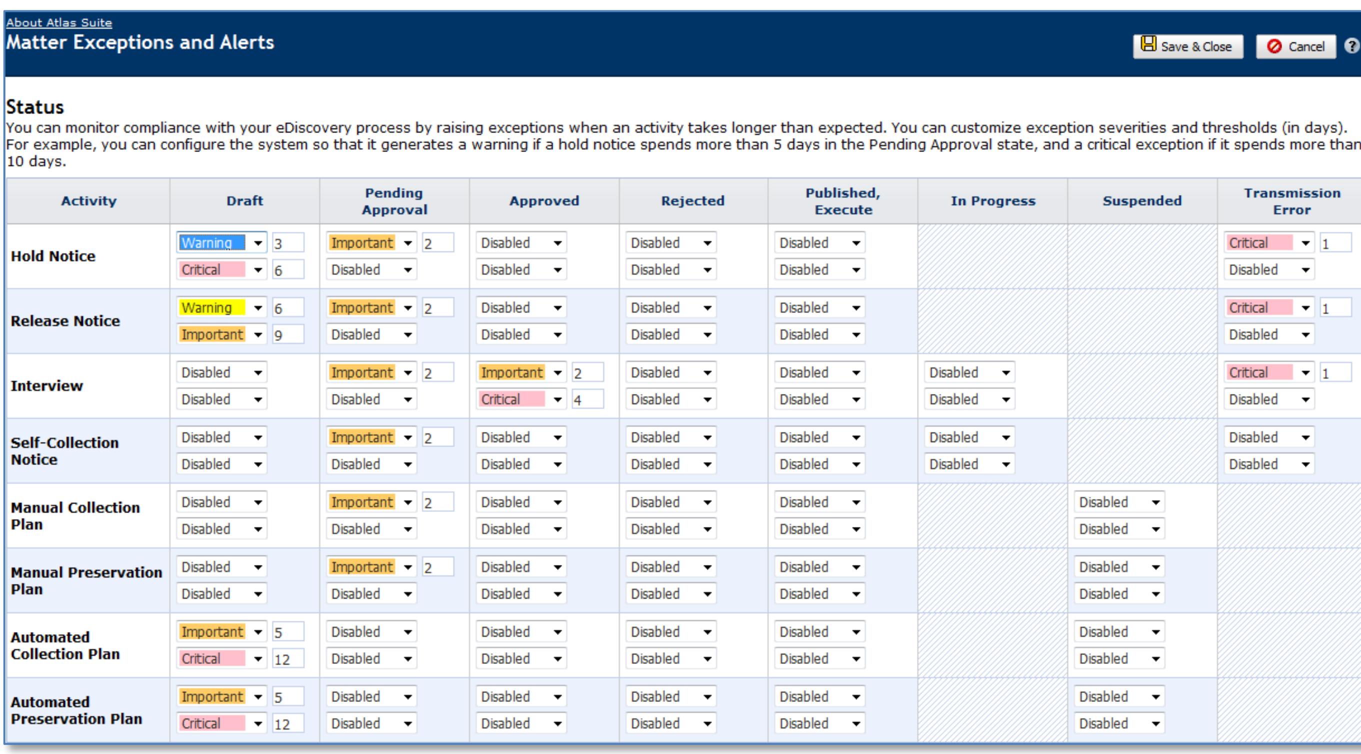
21 Matter Exceptions and Alerts

The **Admin > Matter Exceptions and Alerts** module lets you set the severity of **a)** exceptional states pertaining to Matters and **b)** system Alerts:

- Matter exceptions are time-based measures that detect if a Matter is stalled. For example, if a Notice spends too much time waiting for approval, the Matter's "exception score" is heightened. Legal users can sort the Matters list (in the **Matters** module) based on these scores, allowing them to quickly identify the Matters that need attention. A Matter's details page contains an **Exceptions** tab that lists the individual exceptions for that Matter.
- System Alerts (not just those pertaining to Matters) can be marked as **Warning**, **Important**, or **Critical**. These rankings are used to filter the Alerts that are displayed in a user's **My Alerts** tray on the **My Atlas** page.

21.1 Matter Exceptions

There top two sections of the **Matter Exceptions and Alerts** module let you set the duration threshold and severity of the Matter exceptions. The first section, **Status**, is a grid that displays, right-to-left, the lifecycle states of the various types of Notices and Plans:



Activity	Draft	Pending Approval	Approved	Rejected	Published, Execute	In Progress	Suspended	Transmission Error
Hold Notice	Warning 3 Critical 6	Important 2 Disabled	Disabled Disabled	Disabled Disabled	Disabled Disabled			Critical 1 Disabled
Release Notice	Warning 6 Important 9	Important 2 Disabled	Disabled Disabled	Disabled Disabled	Disabled Disabled			Critical 1 Disabled
Interview	Disabled Disabled	Important 2 Disabled	Important 2 Critical 4	Disabled Disabled	Disabled Disabled	Disabled Disabled		Critical 1 Disabled
Self-Collection Notice	Disabled Disabled	Important 2 Disabled	Disabled Disabled	Disabled Disabled	Disabled Disabled	Disabled Disabled		Disabled Disabled
Manual Collection Plan	Disabled Disabled	Important 2 Disabled	Disabled Disabled	Disabled Disabled	Disabled Disabled		Disabled Disabled	
Manual Preservation Plan	Disabled Disabled	Important 2 Disabled	Disabled Disabled	Disabled Disabled	Disabled Disabled		Disabled Disabled	
Automated Collection Plan	Important 5 Critical 12	Disabled Disabled	Disabled Disabled	Disabled Disabled	Disabled Disabled		Disabled Disabled	
Automated Preservation Plan	Important 5 Critical 12	Disabled Disabled	Disabled Disabled	Disabled Disabled	Disabled Disabled		Disabled Disabled	

Each of the cells in the grid represents a particular state of the Notice or Plan. Each cell contains a two-stage control that lets you set the severity of the situation if the Notice/Plan remains in a state for too long.

For example, when we look at the **Hold Notice/Draft** cell, we see this:

Activity	Draft
Hold Notice	Warning 3 Critical 6

This means that if a Hold Notice remains in **Draft** state for 3 days or more, a **Warning** exception is triggered. If it remains as a **Draft** for 6 days or more, the exception is raised to **Critical**. You don't have to set both stages in a cell; for example, you can declare that a Hold Notice in **Draft** state will trigger a **Critical** exception after 4 days and set the other stage to **Disabled**.

The middle part of the module, **Other**, provides two more Matter exceptions:

Other

Description	Severity / Threshold (days)
No Hold Notices If a matter has no hold notices and is older than 'Threshold', raise an exception.	Important 10 Critical 20
Matter Without Legal Staff If a matter has no attorney or paralegal and is older than 'Threshold', raise an exception.	Important 1 Critical 3

As explained in the UI, the top control lets you set the exception levels if no Hold Notices have been created within certain amounts of time. The bottom control sets the exception levels for Matters that haven't been assigned an Attorney and/or Paralegal, as determined by the **MATTER_NO_ASSIGNEE_CHECK** Parameter in the **MATTER_EXCEPTIONS** Component.

21.1.1 How Matter Exceptions Are Used (and Not Used)

- The Matter list in the **Matters** module gives a count of the number of exceptions the each Matter has incurred. The list can be sorted based on the number of all exceptions or just **Critical** exceptions.
- Each Matter's **Details** page contains an **Exceptions** tab that lists the individual exceptions for the Matter.
- Matter exceptions are *not* Alerts—an email message is *not* sent if a Notice/Plan stays in a state for too long, nor is an entry added to the **My Alerts** tray on the **My Atlas** page. Exceptions are only used to give legal users a measure of a Matter's need for attention.

21.2 Alerts

The **Alert Configuration** section of the page displays a long list of system Alerts:

Alert Configuration

Description	Severity
Others	Warning
An Action Item has been added to a Matter	Warning
An Action Item attached to a Matter has been updated	Warning
An Action Item attached to a Matter has been completed	Warning
A Collection Plan has been routed for approval	Warning
A Preservation Plan has been routed for approval	Warning
A Collection Plan has been approved	Warning
A Collection Plan has been rejected	Important
A Preservation Plan has been approved	Warning
A Hold or Collection Notice has been routed for approval	Warning
A Hold or Collection Notice has been approved	Warning
A Hold or Collection Notice has been rejected	Important
A Virtual Interview Plan has been routed for approval	Warning
A Virtual Interview Plan has been approved	Warning
A Virtual Interview Plan has been rejected	Important
A Retention Schedule has been routed for approval	Warning
An error occurred while routing a Retention Schedule for approval	Critical

All of the system Alerts are listed, and each can be set to one of the three severities. (Unlike with Matter exceptions you can't set an Alert to **Disabled**.) The Alert severities are used as filter settings in the **My Alerts** tray on the **My Atlas** page: A user can ask to see only the **Critical** Alerts, only **Critical and Important**, or **All**.

The Alerts that pertain to Matters are also counted as exceptions in the **Matters** module. For example, if the **Collection Plan has been rejected** Alert is set to **Important** (as shown here), the Matter's exception count is increased when a Collection Plan is rejected. However, it's *only* increased for the recipients of the Alert (the Plan's author and the user who routed the Plan for approval, in this case). Thus, it's possible for different users to see different exception counts for the same Matter.