

## Printed Documentation

---



# Table of Contents

Error! Bookmark not defined.



# Repositories

The Repositories option displays a list of repositories you are authorized to access using the Rights Management Server.

For each repository listed on the left hand side of your screen, you can click it and view NextLabs rights protected and unprotected files.

You can also use the search field to find documents using their name.

## Viewing Files from your Repository

1. Log in to the Rights Management Server portal.
2. Under All Files, select the repositories you want to access.
3. Navigate to your rights protected file.

**NOTE:** You can also type your file name in the Search field.

4. Click the rights protected document to view it in the [Document Viewer](#).

**NOTE:** You can view NextLabs rights protected and unprotected documents in Rights Management Server. All rights protected files are decrypted and then displayed. After you close the file the decrypted file is deleted from Rights Management Server.



# Configuration

The Configuration page allows you to configure settings for the Policy Controller, Mail Server, DropBox App, SharePoint App, Client Management, and other General Settings.

**NOTE:** If you do not intend to use the Document Viewer in your Rights Management Server deployment then you only need to configure the Client Management Settings. Conversely if you do not want to manage any Client devices in your Rights Management Server deployment then you can leave the Client Management Settings blank, while configuring the remaining sections.

The Rights Management Server uses this information to interact with each of these components.

## General Settings

1. In the General Settings section, type the following details:

Field	Description
Session Timeout	Type the minimum number of minutes before your Rights Management Server web portal session is terminated.
Turn on User Location	Set this field to <b>Yes</b> if you want to enforce policies that allow or deny access to NextLabs rights protected documents.
Policy User Location Identifier	This is the attribute name used in your policies to specify the country code of the user for whom you want to allow or deny access to a NXL protected document.
Location DB Last identified time	<p>This displays the last time the Location database file was updated.</p> <p><b>NOTE:</b> This file is used for location lookup of the IP address that accompanies a user request to access a NXL protected document.</p>
Location Update Frequency	<p>This is the frequency of update performed for the Location database file.</p> <p><b>NOTE:</b> The first time you set this option, Rights Management Server downloads the Location database file for the first time. If your Internet connection speed is slow, then the Rights Management Server user interface (for the current session) may become non-responsive until the Location database file has been downloaded.</p>

2. Click **Save**.

**NOTE:** After you have configured the User Location settings, in your Tomcat Server you must set the JAVA\_OPTS parameter value in the catalina.bat file. For more information, refer to the User Location Settings section in the Rights Management Server Administrator's Guide.

## Client Management Settings

1. In the Client Management Settings section, enter the following details:

Field	Description
ICENet Server URL	This is the IP Address or the fully qualified domain name (FQDN) of the web services URL.
Client Version Number	<p>This is the version number of the latest Rights Management Client (RMC) installation file.</p> <p>The Rights Management Client deployed on different machines checks against this Client Version Number to determine if a new version of the RMC installer is available.</p>
Client Package Download URL (32-bit)	<p>This is the URL that is used to download the 32-bit version of the Rights Management Client (RMC) installer.</p> <p>This is the location from where the RMC downloads the new installer.</p>
Client Package Checksum (32-bit)	<p>This is the Check value which is associated with the 32-bit installation file.</p> <p>This value can be generated by using the appropriate Checksum tools on the new installation file.</p>
Client Package Download URL (64-bit)	<p>This is the URL that is used to download the 64-bit version of the Rights Management Client (RMC) installer.</p> <p>This is the location from where the RMC downloads the new installer.</p>
Client Package Checksum (64-bit)	<p>This is the Check value which is associated with the 64-bit installation file.</p> <p>This value can be generated by using the</p>



appropriate Checksum tools on the new installation file.

2. Click **Save**.

## Mail Server Settings

1. In the Mail Server Settings section, set **Allow Registration Request** to **Yes**.
2. Enter the following details:

Field	Description
SMTP Host	This is the hostname of your SMTP Mail Server  <b>NOTE:</b> If your Rights Management Server is deployed on a Linux system then you must specify the corresponding IP Address for this field.
SMTP Port	This is the port number at which Rights Management Server and SMTP communication occurs.
SMTP Authentication needed?	If you want to enable SMTP authentication prior to any email being sent due to Rights Management Server, then select Yes
SMTP User Name	This is the user name for the mail account which will send emails to the Administrator and sponsor on behalf of Rights Management Server.
SMTP Password	This is the password for the SMTP User Name
Reenter SMTP Password	Confirm your SMTP Password
Enable TLS?	Transport Layer Security (TLS) is a protocol that encrypts and delivers messages in a secure fashion. If you want to use this protocol for communication between the Rights Management Server and your SMTP mail server then select True.
Email Subject	This is the subject of the email that the SMTP mail server sends on behalf of Rights Management Server. You can specify this to be something meaningful that would indicate the purpose of the email to be related to Rights Management Server user

	account creation.
Rights Management Server Administrator Email	This is the email address of the Administrator that you want to send the user account creation request email to.

3. Click **Save**.

## Policy Controller Settings

The Policy Controller Settings are used by the Rights Management Server to communicate with the Policy Controller in order to determine if a User has sufficient Rights to view a file in Document Viewer.

1. In the Policy Controller Settings section, type the following details:

- 1.

Field	Description
Policy Controller Hostname	<p>hostname of the machine your Policy Controller's Key Management and Policy Evaluation component is installed on.</p> <p>This must be specified in the following format: https://&lt;server name&gt;:&lt;port number&gt;</p> <p>For example: https://RightsManagement.mycompany.com:8443</p> <p><b>NOTE:</b> If your Rights Management Server is deployed on a Linux system then you must specify the corresponding IP Address for this field.</p>
RMI Port Number for Key Management	port number on which Rights Management Server communicates with the Policy Controller for the purpose of Key Management
KeyStore file	<p>complete file path for the KeyStore file. This file has the certificate that is used to identify Rights Management Server to the Policy Controller.</p> <p><b>NOTE:</b> The certificate in this KeyStore should be imported into the TrustStore of the Policy Controller, which is specified in the Key Management Service Plugin of the Policy Controller.</p>
KeyStore Password	password for the KeyStore
TrustStore File	complete file path for the TrustStore file. This file

	includes the certificates that are trusted by Rights Management Server.
TrustStore Password	password for the TrustStore
RMI Port Number for Policy Evaluation	port number on which Rights Management Server communicates with the Policy Controller for the purpose of Policy Evaluation

- Click **Test Connection** to verify that the Rights Management Server can connect to the Policy Controller connection details.
- Click **Save**.

## DropBox App Settings

- In the DropBox App Settings section, set **Allow Personal Repositories** to **Yes**.  
**NOTE:** The following Dropbox App Settings can only be obtained after a Dropbox App has been created for Rights Management Server. For more details, refer to the Rights Management Server Installation Guide.
- Type the following details:

Field	Description
Dropbox App Key	this value is used by Rights Management Server to establish a secure communication channel with Dropbox
Dropbox App Secret	this value is used by Rights Management Server to establish a secure communication channel with Dropbox
Dropbox Redirect URL	URL used by users to access the Rights Management Server portal

- Click **Save**.

## SharePoint App Settings

- In the SharePoint App Settings section, click **Add SharePoint Application**.
- Complete the following details:

Field	Description
SharePoint Type	Select the type of SharePoint deployment you are creating your SharePoint for. SharePoint Online (cloud based) or SharePoint On-Premise (stand alone deployment on your company's intranet).
Display Name	











	this is the displayed name for the SharePoint App you want to configure.
Remote App URL ( <b>NOTE:</b> This field is visible only if you have selected SharePoint Type as SharePoint On-Premise)	<p>this is the URL of your SharePoint On-Premise web application that you have deployed on your IIS. You must append the following to it: /Pages/Default.aspx For example if your SharePoint Site App URL is: https://myserver:4444 then you must type it as: https://myserver:4444/Pages/Default.aspx <b>NOTE:</b> If you have not changed the default port number (443) for your server then you don't need to specify the port number in the URL. Therefore, the above URL would be listed as: https://myserver/Pages/Default.aspx</p>
App Client ID	this is the value generated by SharePoint when you registered your SharePoint Application. For more details, see Registering your SharePoint Online Application in the Rights Management Server Administrator Guide.
App Client Secret	this is the value generated by SharePoint when you registered your SharePoint Application. For more details, see Registering your SharePoint Online Application in the Rights Management Server Administrator Guide.

3. Click **Save**.











4. Click the download icon .

# Document Viewer








The Document Viewer opens in a new web browser window when you click NextLabs rights protected file listed under your listed repository. You can use the following options to view your NextLabs rights protected document in the Document Viewer:












Feature	Description
	Click to navigate to the previous page.
	Click to navigate to the next page.
	Click to fit your document vertically in the document viewer
	Click to fit your document horizontally in the document viewer
	Click to rotate your document anticlockwise.
	Click to rotate your document clockwise.
	Click to zoom in to your document. <b>NOTE:</b> The pinch zoom gesture is disabled for NXL protected documents that are viewed on a mobile device. You can instead use this icon to zoom in on your screen.
	Click to zoom out of your document. <b>NOTE:</b> The pinch zoom gesture is disabled for NXL protected documents that are viewed on a mobile device. You can instead use this icon to zoom out on your screen.
	Click to print your document. <b>NOTE:</b> You can only print a document if you have sufficient permission. This icon is not visible if you are viewing your document using a mobile web browser.
	Click to view the file type, size, classification labels, and file rights such as print, view, etc.

If you are viewing a VDS file, then you can use the following options:

Feature	Description
	Click to toggle the display of each steps's description.
	Click to return to the first step.
	Click to play the current step.
	Click to pause at the current step
	Click to play all steps from step1 onwards.
	Click to print the current view of your VDS file.  <b>NOTE:</b> You can only print if you have sufficient permission. This icon is not visible if you are viewing your document using a mobile web browser.
	Click to download a rights protected file.
	Click to view the file type, size, classification labels, and file rights such as print, view, etc.
	Click the arrow to view the next scene.
	Click the arrow to view the previous scene.

If you are viewing a CAD file, you can use the following options:

Feature	Description
	Click to return to the view that was originally displayed before you entered the 3D navigation mode.
	Click to view different views such as top view, left view, back view, front view, right view, and ISO view of the 3D file.
	Wireframe - Displays objects using lines and curves to represent the boundaries.
	Shaded- Displays objects using smooth shading
	Wireframe on Shaded- Superimposes a wireframe display on all shaded objects in a view
	Hidden Line Mode - Displays objects using wireframe representation and hides lines representing back faces.
	Click to measure the distance between two points.  Click on any area of your model and click a second time to mark the second point to which you want to measure.

	<p><b>NOTE:</b> Each measurement you make on your model is represented in the Model Browser window, under <b>Measurements</b>. You can select each measurement to view it on your model and also toggle it from view.</p>
	<p>Click to measure the angle between two points.</p> <p><b>NOTE:</b> Each measurement you make on your model is represented in the Model Browser window, under <b>Measurements</b>. You can select each measurement to view it on your model and also toggle it from view. This option does not work for all types of models.</p>
	<p>Click to select a part.</p> <p>The part is highlighted in green color and is also selected in the Model Browser window.</p> <p><b>NOTE:</b> Select a part in the Model Browser window and it is highlighted in the display area.</p>
	Click to measure distance between faces
	Turntable - Click to rotate the image 2D.
	Orbit Camera - Click to rotate the image 3D.
	Walk - Enables walk through a model at a fixed height above the XY plane, by dynamically controlling the location and target of the camera
	Explode - Move the slider to break a compound object into its component objects.
	Cutting Plane - Move the slider to cut plane for each display configuration in a drawing.
	<p><b>Settings</b> - Allows you to configure the background color, projection mode, and measurement color.</p> <p><b>Orbit and Turntable Momentum</b> - If you enable this option, and then rotate the image, the object will continue rotating until you click on the screen.</p> <p><b>Projection Mode</b> - Select the <b>Orthographic</b> or <b>Perspective</b> mode.</p> <p><b>Show Backfaces</b> - Select this option, if you want to include back faces.</p>
	Click to print the current view of the CAD file
	Click to view the file type, size, classification

labels, and file rights such as print, view, etc.

## Model Browser

The Model Browser is displayed in the Document Viewer when you are viewing JRT or PRT files. It contains a list of all the parts that are displayed in the Document Viewer. You can toggle each part and subpart of your model from view.

The Model Browser also lists all measurement annotations (the distance between two points and the angle between two points) under a **Measurements** section. These annotations can also be toggled from view.

## Properties window

The Properties window displays when you select a particular part in your model. It displays the **Name** of the part and the part's **Parent**.

In the Properties window, you can use the following options for the selected part:

Option	Description
<b>Parent</b>	Click to select the parent of the selected part.
<b>Transparency</b>	Click to view the transparent version of the selected part.
<b>Bounding Box</b>	Click to view the bounding box dimensions of the selected part.

### CONFIDENTIALITY NOTICE

THIS DOCUMENT IS CONFIDENTIAL AND PROPRIETARY TO NEXTLABS, INC. AND MAY NOT BE REPRODUCED, PUBLISHED OR DISCLOSED TO OTHERS WITHOUT COMPANY AUTHORIZATION.

© 2014 - 2016 NextLabs, Inc. All Rights Reserved



# Manage Repositories

Rights Management Server allows you to add personal repositories to view or download NextLabs rights protected documents and unprotected documents. The documents in the repository cannot be edited and you cannot upload a document to the repository.

## Adding a Personal Repository

1. Go to **Manage Repositories**.
2. Click **Add Repository**.
3. Select a service provider from the list.
4. Enter your repository **Display Name**.
5. If you selected SharePoint On Premise or SharePoint Online as the service provider, enter the site address.
6. Click **CONNECT**.

## Editing a Repository

1. Move the cursor over the repository.
2. Click the **Edit** icon.
3. Edit the **Display Name**
4. Click **Save**.

## Deleting a Repository

1. Move the cursor over the repository.
2. Click the **Delete** icon.
3. Click **OK**, in the confirmation dialog box.



# Upload & View

Rights Management Server allows users to upload and view NextLabs rights protected documents and unprotected documents in a secure manner. [Click here](#) for the list of supported formats. RMS interacts with the Policy Controller before it displays any rights protected content for a user. If you are not authorized to view the document you have uploaded, Rights Management Server displays a message indicating this.

Perform the following steps to view the document:

1. Login to the Rights Management Server portal.
2. Click **Upload**.
3. Click **Browse** and select your rights protected document.
4. Click **Open**.



# Downloading the Rights Management Client

Rights Management Client (RMC) allows you to protect and classify documents. RMC enforces your company's information governance policies based on your user credentials. These include not only user attributes but also the classification labels attached to documents, and environmental context (such as which computer the user is logged on from).

In the Rights Management Client, with the appropriate rights the user can view not only a rights protected document but also print, edit, and taking screen shots of the document.

In NextLabs Rights Management Server users can download the NextLabs Rights Management Client (RMC) installation package via RMS. However, to make the Rights Management Client installation package available for download, administrator must configure it. See **NextLabs Rights Management Server, Administrator's Guide** for steps for configuring Rights Management Client.

To download NextLabs Rights Management Client:

1. Log into the Rights Management Server.
2. Scroll to the bottom of a screen.
3. Click **Download Rights Management Client**.



# Key Management

RMS allows you to generate keys for encrypting/decrypting the files. These keys are downloaded by the client application for encrypting/decrypting the files.

Click **GENERATE KEY** to generate a key. Any existing keys will be obsolete.





# Configuration

The Configuration page allows you to configure settings for the Policy Controller, Mail Server, DropBox App, SharePoint App, Client Management, and other General Settings.

**NOTE:** If you do not intend to use the Document Viewer in your Rights Management Server deployment then you only need to configure the Client Management Settings. Conversely if you do not want to manage any Client devices in your Rights Management Server deployment then you can leave the Client Management Settings blank, while configuring the remaining sections.

The Rights Management Server uses this information to interact with each of these components.

## General Settings

1. In the General Settings section, type the following details:

Field	Description
Session Timeout	Type the minimum number of minutes before your Rights Management Server web portal session is terminated.
Turn on User Location	Set this field to <b>Yes</b> if you want to enforce policies that allow or deny access to NextLabs rights protected documents.
Policy User Location Identifier	This is the attribute name used in your policies to specify the country code of the user for whom you want to allow or deny access to a NXL protected document.
Location DB Last identified time	<p>This displays the last time the Location database file was updated.</p> <p><b>NOTE:</b> This file is used for location lookup of the IP address that accompanies a user request to access a NXL protected document.</p>
Location Update Frequency	<p>This is the frequency of update performed for the Location database file.</p> <p><b>NOTE:</b> The first time you set this option, Rights Management Server downloads the Location database file for the first time. If your Internet connection speed is slow, then the Rights Management Server user interface (for the current session) may become non-responsive until the Location database file has been downloaded.</p>

2. Click **Save**.

**NOTE:** After you have configured the User Location settings, in your Tomcat Server you must set the JAVA\_OPTS parameter value in the catalina.bat file. For more information, refer to the User Location Settings section in the Rights Management Server Administrator's Guide.

## Client Management Settings

1. In the Client Management Settings section, enter the following details:

Field	Description
ICENet Server URL	This is the IP Address or the fully qualified domain name (FQDN) of the web services URL.
Client Version Number	<p>This is the version number of the latest Rights Management Client (RMC) installation file.</p> <p>The Rights Management Client deployed on different machines checks against this Client Version Number to determine if a new version of the RMC installer is available.</p>
Client Package Download URL (32-bit)	<p>This is the URL that is used to download the 32-bit version of the Rights Management Client (RMC) installer.</p> <p>This is the location from where the RMC downloads the new installer.</p>
Client Package Checksum (32-bit)	<p>This is the Check value which is associated with the 32-bit installation file.</p> <p>This value can be generated by using the appropriate Checksum tools on the new installation file.</p>
Client Package Download URL (64-bit)	<p>This is the URL that is used to download the 64-bit version of the Rights Management Client (RMC) installer.</p> <p>This is the location from where the RMC downloads the new installer.</p>
Client Package Checksum (64-bit)	<p>This is the Check value which is associated with the 64-bit installation file.</p> <p>This value can be generated by using the</p>

appropriate Checksum tools on the new installation file.

2. Click **Save**.

## Mail Server Settings

1. In the Mail Server Settings section, set **Allow Registration Request** to **Yes**.
2. Enter the following details:

Field	Description
SMTP Host	This is the hostname of your SMTP Mail Server  <b>NOTE:</b> If your Rights Management Server is deployed on a Linux system then you must specify the corresponding IP Address for this field.
SMTP Port	This is the port number at which Rights Management Server and SMTP communication occurs.
SMTP Authentication needed?	If you want to enable SMTP authentication prior to any email being sent due to Rights Management Server, then select Yes
SMTP User Name	This is the user name for the mail account which will send emails to the Administrator and sponsor on behalf of Rights Management Server.
SMTP Password	This is the password for the SMTP User Name
Reenter SMTP Password	Confirm your SMTP Password
Enable TLS?	Transport Layer Security (TLS) is a protocol that encrypts and delivers messages in a secure fashion. If you want to use this protocol for communication between the Rights Management Server and your SMTP mail server then select True.
Email Subject	This is the subject of the email that the SMTP mail server sends on behalf of Rights Management Server. You can specify this to be something meaningful that would indicate the purpose of the email to be related to Rights Management Server user

	account creation.
Rights Management Server Administrator Email	This is the email address of the Administrator that you want to send the user account creation request email to.

3. Click **Save**.

## Policy Controller Settings

The Policy Controller Settings are used by the Rights Management Server to communicate with the Policy Controller in order to determine if a User has sufficient Rights to view a file in Document Viewer.

1. In the Policy Controller Settings section, type the following details:

- 1.

Field	Description
Policy Controller Hostname	<p>hostname of the machine your Policy Controller's Key Management and Policy Evaluation component is installed on.</p> <p>This must be specified in the following format: https://&lt;server name&gt;:&lt;port number&gt;</p> <p>For example: https://RightsManagement.mycompany.com:8443</p> <p><b>NOTE:</b> If your Rights Management Server is deployed on a Linux system then you must specify the corresponding IP Address for this field.</p>
RMI Port Number for Key Management	port number on which Rights Management Server communicates with the Policy Controller for the purpose of Key Management
KeyStore file	<p>complete file path for the KeyStore file. This file has the certificate that is used to identify Rights Management Server to the Policy Controller.</p> <p><b>NOTE:</b> The certificate in this KeyStore should be imported into the TrustStore of the Policy Controller, which is specified in the Key Management Service Plugin of the Policy Controller.</p>
KeyStore Password	password for the KeyStore
TrustStore File	complete file path for the TrustStore file. This file

	includes the certificates that are trusted by Rights Management Server.
TrustStore Password	password for the TrustStore
RMI Port Number for Policy Evaluation	port number on which Rights Management Server communicates with the Policy Controller for the purpose of Policy Evaluation

- Click **Test Connection** to verify that the Rights Management Server can connect to the Policy Controller connection details.
- Click **Save**.

## DropBox App Settings

- In the DropBox App Settings section, set **Allow Personal Repositories** to **Yes**.  
**NOTE:** The following Dropbox App Settings can only be obtained after a Dropbox App has been created for Rights Management Server. For more details, refer to the Rights Management Server Installation Guide.
- Type the following details:

Field	Description
Dropbox App Key	this value is used by Rights Management Server to establish a secure communication channel with Dropbox
Dropbox App Secret	this value is used by Rights Management Server to establish a secure communication channel with Dropbox
Dropbox Redirect URL	URL used by users to access the Rights Management Server portal

- Click **Save**.

## SharePoint App Settings

- In the SharePoint App Settings section, click **Add SharePoint Application**.
- Complete the following details:

Field	Description
SharePoint Type	Select the type of SharePoint deployment you are creating your SharePoint for. SharePoint Online (cloud based) or SharePoint On-Premise (stand alone deployment on your company's intranet).
Display Name	

	this is the displayed name for the SharePoint App you want to configure.
Remote App URL ( <b>NOTE:</b> This field is visible only if you have selected SharePoint Type as SharePoint On-Premise)	<p>this is the URL of your SharePoint On-Premise web application that you have deployed on your IIS. You must append the following to it: /Pages/Default.aspx For example if your SharePoint Site App URL is: https://myserver:4444 then you must type it as: https://myserver:4444/Pages/Default.aspx <b>NOTE:</b> If you have not changed the default port number (443) for your server then you don't need to specify the port number in the URL. Therefore, the above URL would be listed as: https://myserver/Pages/Default.aspx</p>
App Client ID	this is the value generated by SharePoint when you registered your SharePoint Application. For more details, see Registering your SharePoint Online Application in the Rights Management Server Administrator Guide.
App Client Secret	this is the value generated by SharePoint when you registered your SharePoint Application. For more details, see Registering your SharePoint Online Application in the Rights Management Server Administrator Guide.

3. Click **Save**.

4. Click the download icon .

# Manage Repositories

This page allows you to add shared and personal repositories.

- **Shared** - Multiple users can use the same repository.
- **Personal** - The repository is dedicated to a single user.

You can add repositories after they are configured in the **System Settings > Configured Providers**. Each repository lists the rights protected and unprotected files present in it.

## Adding a Shared Repository

1. Go to **Manage Repositories**.
2. Click **Add Repository**.
3. Select **SharePoint** or **SharePoint Online** as the service provider from the list.
4. Enter your repository **Display Name**.
5. Enter the site address.
6. Click **CONNECT**.

## Adding a Personal Repository

1. Go to **Manage Repositories**.
2. Click **Add Repository**.
3. Select a service provider from the list.
4. Enter your repository **Display Name**.
5. Enter the site address.
6. Click **CONNECT**.
7. Click **Allow** to grant Rights Management Server access to the files and folders in your Dropbox, Google Drive, or One Drive account.

## Updating a Repository

1. Move the cursor over the repository.
2. Click the **Edit** icon.
3. Update the display name.
4. Click **SAVE**.

## Deleting a Repository

1. Move the cursor over the repository.
2. Click the **Delete** icon for the repository you want to remove.
3. Click **OK**, in the confirmation dialog box.





# Rights Management Server

Rights Management Server allows you to view NextLabs rights protected documents in your repositories via a web portal. It also allows you to upload rights protected documents and view them in your web browser.

Rights Management Server decrypts the file and displays it. After you are done viewing it the file is deleted. Rights Management Server does not retain any rights protected document on the server. Files in your repository are not edited or deleted.

You can also authorize trusted business partners that exist outside of your company intranet to view confidential information that you want to collaborate with them on.

## Logging in to the Rights Management Server web portal

1. Type the URL for your Rights Management Server in your web browser's address bar.

**NOTE:** If you are using Internet Explorer to access the Rights Management Server portal then you must add the URL as a Trusted Site in Internet Explorer. This allows JavaScript execution when you access the Rights Management Server portal. If you are using Internet Explorer 9 then you must switch off compatibility view to allow the user interface to render properly.

2. Type your login credentials.
3. Select the domain you want to login to.
4. Click **LOGIN**.

## Requesting a Rights Management Server User Account

If your Rights Management Server deployment has not been enabled for allowing registration requests, then you cannot request a User Account.

1. In the Rights Management Server login page, click **Request an Account**.
2. Type the following details:

- **First Name:** Your first name.
- **Last Name:** Your last name.
- **Email ID:** Your email address.
- **Company:** Your Company's name.
- **Sponsor:** The name of the sponsor who wants to share documents with you.

- **Sponsor's Email Address:** Your sponsor's email address.
  - **Reason for request:** Given reason for requesting access. Please specify the purpose and nature of your collaboration with your sponsor.
3. Click **Request an account**.

# Contact Us

For troubleshooting any issues related to your Rights Management Server software email support at [support@nextlabs.com](mailto:support@nextlabs.com).



# Index

## A

Active Directory 7, 25

Add 33

URL 33

## B

Browse 19

## C

Company's 33

Contact Us 35

## D

Deployed 19

Policy Controller 19

Document Viewer 13

## E

Email 33, 35

Email ID 33

## F

First Name 33

## I

Internet Explorer 33

## J

JavaScript 33

## L

Last Name 33

## M

Manage Repositories 31

## N

Nextlabs 35

NOTE 33

Nxl 31

Nxl file 5

## P

Policy Controller 7, 19, 25

## R

Register 33

Repositories 5

Requesting 33

RMS User Account 33

Rights Management Server 5, 7, 25, 33

RMS 5, 7, 19, 25, 33, 35

RMS User Account 33

Requesting 33

## S

Search 5

Settings 7, 25

Sign 33

Sponsor's Email Address 33

## T

Techpubs 35

Trusted Site 33

## U

Unencrypted 5

Upload 19

URL 33

Using

Rights Management Server 5

## V

View 19