



**NEXTLABS<sup>®</sup>**

## **Rights Management Server**



**Administrator's Guide**

**Release 8.3**

**January 2016**



---

Copyright © 2009-2016 NextLabs, Inc. All rights reserved.  
The information in this document is subject to change without notice.

NextLabs welcomes comments or suggestions regarding this manual or any of our product documentation. Please send an e-mail to [info@nextlabs.com](mailto:info@nextlabs.com).

## TRADEMARKS

NextLabs<sup>®</sup>, ACPL<sup>®</sup>, RMS<sup>™</sup>, and the RMS logo are registered trademarks of NextLabs, Inc. All other brands or product names used herein are trademarks or registered trademarks of their respective owners.

## LICENSE AGREEMENT

This documentation and the software described in this document are furnished under a license agreement or nondisclosure agreement. The documentation and software may be used or copied only in accordance with the terms of those agreements. No part of this manual may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's use, without the prior written permission of NextLabs, Inc.

The content of this manual is provided for informational and instructional use only. It is subject to change without notice, and should not be construed as a commitment by NextLabs, Inc.

NextLabs, Inc. assumes no responsibility or liability for any inaccuracies or technical errors that may appear in the content of this manual.

Published in San Mateo, CA, by NextLabs, Inc.  
[www.nextlabs.com](http://www.nextlabs.com)  
[info@nextlabs.com](mailto:info@nextlabs.com)  
650.577.9101

Document Revision Number: RMS-8.3

---




<b>1. Introduction</b>	<b>7</b>
Welcome	7
Inside this Administrator Guide	7
Introducing Rights Management Server	9
Conventions used in this Document	9
Key Benefits	10
RMS and RMC	10
Logical Architecture	12
Support for NXL Protected Documents	13
<b>2. Installing Rights Management Server</b>	<b>15</b>
Installing Rights Management Server	15
Before You Start	16
Prerequisites	16
Supported Platforms	16
NextLabs Software	16
Supported Databases	16
Supported Web Browsers	18
Supported File Formats	19
Database for Location lookup	20
Installing Rights Management Server	21
Installing Viewers	21
License Key File	21
Running the Installation Wizard	21
Running a Silent Installation	26
Logging in to the Rights Management Server Portal	29
Minimum Screen Resolution	29

Accessing Rights Management Server using Internet Explorer . . . . .	30
Uninstalling Rights Management Server . . . . .	33
Running the Uninstallation Wizard . . . . .	33
Performing a silent Uninstallation . . . . .	33
Uninstalling Viewers . . . . .	35
Uninstalling Document Viewer . . . . .	35
Uninstalling CAD Viewer . . . . .	35
Uninstalling SAP Viewer . . . . .	35
Upgrading Rights Management Server from 8.0/8.1 to 8.3 . . . . .	36
Starting/Stopping/Restarting RMS Service . . . . .	37
<b>3. Configuring Rights Management Server . . . . .</b>	<b>39</b>
Configuring Rights Management Server . . . . .	39
Configuring your Java Policy Controller . . . . .	40
Configuring Remote Java Policy Controller Communication . . . . .	41
KeyStore & TrustStore Files . . . . .	41
Generating the Certificate . . . . .	42
Exporting the Certificate . . . . .	43
Importing the Certificate into the TrustStore . . . . .	43
Adding Attributes to the KeyManagement Services File . . . . .	43
. . . . .	44
Configuring a NXL Filter for MS SharePoint. . . . .	45
Specifying the NXL File Type. . . . .	45
Specifying NXL Registry Entries . . . . .	45
Configuring Alternate Access Mapping . . . . .	47
Configuring Alternate Access Mappings in Sharepoint 2010 and 2013. . . . .	47
Configuring Logging . . . . .	49
Configuring Service Providers . . . . .	50
Configuring the Remote Policy Controller Settings . . . . .	51
Configuring the Mail Server Settings . . . . .	53
Configuring Client Management Settings. . . . .	55
Configuring User Location Settings . . . . .	56
Other Configuration Parameters . . . . .	57
Configuring Watermark Information . . . . .	58
Policy based Watermark . . . . .	58
Config File based Watermark . . . . .	61
Policy versus Config File based Watermark . . . . .	62
Configuring the Session Timeout Duration . . . . .	63
Configuring Rights for Control Center . . . . .	64

Configuring Rights Management Obligation . . . . .	65
Configuring the Rights Management Client . . . . .	66
Specifying the RMC package location . . . . .	66
Downloading the Rights Management Client . . . . .	66
Configuring RMC_Classification.xml . . . . .	66
Configuring Local or External Login Credentials for RMC . . . . .	66
Configuring RMS Memory Settings . . . . .	68
Importing Your Own SSL Certificates for Rights Management Server . . . . .	69
<b>4. Repositories . . . . .</b>	<b>71</b>
Adding a Repository . . . . .	71
Integrating with SharePoint . . . . .	73
Exporting a Self-Signed Certificate to Rights Management Server . . . . .	74
<b>5. Integrating with SharePoint Online . . . . .</b>	<b>79</b>
Introduction . . . . .	79
Registering your SharePoint Online App . . . . .	80
Creating your SharePoint Online App . . . . .	82
Deploying your SharePoint Online App . . . . .	83
Removing an Expired Client Id and Certificate Name . . . . .	84
<b>6. Integrating with SharePoint On-Premise . . . . .</b>	<b>85</b>
Introduction . . . . .	85
Deploying the Provider Hosted App . . . . .	87
Prerequisites . . . . .	87
Registering the High-Trust App . . . . .	87
Configure the Remote Web Server with the Certificate . . . . .	87
Importing the .pfx Certificate . . . . .	88
Importing the .cer Certificate . . . . .	88
Configuring SharePoint to Use the Certificate . . . . .	89
Distributing the .cer file to SharePoint . . . . .	89
Configuring the Certificate . . . . .	89
Modifying the SetParameters File . . . . .	90
Modifying your Web Server's web.config File . . . . .	91
Publishing Remote Web App in SharePoint . . . . .	91
Configuring Protocol Binding for the Web App . . . . .	92
Configuring Authentication for the Web App . . . . .	92
Creating your SharePoint On-Premise Apps . . . . .	93
<b>7. Integrating with Dropbox . . . . .</b>	<b>95</b>
Configuring Rights Management Server . . . . .	95
Configuring Rights Management Server for Dropbox Repositories . . . . .	96


Creating your Dropbox App for Rights Management Server .....	96
Configuring your Dropbox App. ....	98
<b>8. Integrating with Google Drive .....</b>	<b>101</b>
Configuring Rights Management Server .....	101
Configuring Rights Management Server for Google Drive .....	102
Creating your Google Drive App for Rights Management Server .....	102
Configuring your Google Drive App .....	105
<b>9. Integrating with Microsoft OneDrive .....</b>	<b>107</b>
Configuring Rights Management Server .....	107
Configuring Rights Management Server for Microsoft OneDrive .....	108
Creating your OneDrive App for Rights Management Server .....	108
Configuring your OneDrive App .....	109
<b>10. Access Control using Policies .....</b>	<b>111</b>
Granting Rights to Users .....	111
Enforcing IP Address Policies .....	112
Enforcing Physical Location Policies .....	113
Inserting Hyperlinks in your Policy Obligation .....	114
Defining Application name in policies for RMS .....	115
<b>11. Troubleshooting .....</b>	<b>117</b>
FAQs .....	117
UI Display Problems .....	119
SSL Certificate Exceptions .....	120
Internet Protocol (IP) and Hostname Mismatch .....	120
Importing a Self Signed Certificate for the User .....	120


### Welcome

Rights Management Server is a web based solution that enables your NextLabs (NXL) protected documents to be  viewed by authorized users without the need to install any proprietary NextLabs software. Rights Management Server allows you to collaborate with external business partners without worrying about unauthorized users viewing content that is considered sensitive.


Companies host sensitive information internally through sites which can be accessed by their employees. In order to maintain the privacy and integrity of information that is classified as sensitive, it is important to rely on a mechanism that can extend information security beyond the company intranet.

Encrypting sensitive information is one of the ways you can support the effort to protect information from unauthorized access.

Rights Management Server allows authorized personnel to view NXL protected documents through its web based viewer. 

If the User  wants to edit a NXL protected document, then Rights Management Server also makes the NextLabs Rights Management Client installation package available for download.


The Rights Management Client (RMC)  enables Users who have sufficient Rights to view pdf and office documents in their respective native applications in a secure manner.

In the RMC, with the appropriate Rights the User can not only view a NXL protected document but also do more. This includes but is not limited to  making copies, printing, editing, and taking screen shots of the document.

### Inside this Administrator Guide

This user guide provides information for Rights Management Server which is presented in the following sections:

- [Introducing Rights Management Server](#) elaborates on the key benefits of Rights Management Server, its Logical Architecture, and how Rights Management Server and NextLabs components are integrated during a policy evaluation.
- [Installing Rights Management Server](#) describes how to install Rights Management Server.

- [Configuring Rights Management Server](#) describes configuration steps for connecting to the Policy Controller, Mail Server, Logging, and other configuration parameters. These will vary from customer to customer, based on your implementation.
- [Repositories](#) describes how to add a Repository and exporting a self signed certificate for a demo setup of Rights Management Server.
- [Integrating with SharePoint Online](#) describes how to integrate your Rights Management Server deployment with Microsoft SharePoint Online.
- [Integrating with SharePoint On-Premise](#) describes how to integrate your Rights Management Server deployment with Microsoft SharePoint On-Premise.
- [Integrating with Dropbox](#) describes the steps involved setting up Dropbox access for your Rights Management Server deployment.
- [Integrating with Google Drive](#) describes the steps involved setting up Google Drive access for the Rights Management Server deployment.
- [Troubleshooting](#) contains a FAQ  and different scenarios that might be frequently encountered along with their suggested solutions.



## Introducing Rights Management Server

This section introduces you to the key features of Rights Management Server. It covers the following information:

- [Key Benefits](#)
- [Logical Architecture](#)


## Conventions used in this Document

The following usage conventions occur in this document:

Term	Description
<RMS_DATA_DIR>	<p>You can specify the path to save Rights Management Server data at the time of installation. If you do not specify the Rights Management Server data directory then the default locations for &lt;RMS_DATA_DIR&gt; are:</p> <ul style="list-style-type: none"> <li>• <b>Windows Deployment:</b> C:\ProgramData\NextLabs\RMS\datafiles</li> <li>• <b>Linux Deployment:</b> /var/opt/nextlabs/RMS/datafiles</li> </ul> <p>The Rights Management Server Data Directory contains files like config file, log file, etc. The <code>RMSConfig.properties</code> file contains details about the Active Directory.</p> <p><b>NOTE:</b> It is not mandatory to set a new Rights Management Server data directory. It is recommended not to set a new directory path explicitly unless necessary.</p>
<RMS_INSTALL_DIR>	<p>You can specify the path to install Rights Management Server at the time of installation. If you do not specify the install location then the default locations for &lt;RMS_INSTALL_DIR&gt; are:</p> <ul style="list-style-type: none"> <li>• <b>Windows Deployment:</b> C:\Program Files\NextLabs\RMS\</li> <li>• <b>Linux Deployment:</b> /opt/nextlabs/RMS/</li> </ul>

---

## Key Benefits

NextLabs Rights Management Server is a web based solution that allows authorized users to view NXL protected documents without the need for installing proprietary software. 

Rights Management Server allows you to collaborate with employees inside or outside your company when it comes to your confidential and sensitive information assets. Global collaboration and distributed work environments are a reality for every transcontinental company. However, the mandated requirements for maintaining data confidentiality and integrity in such an environment can prohibit business operations from fulfilling their purpose.



Contemporary information risk solutions involve the deployment of a common software layer which regulates access to confidential information. This approach works well for internal consumption and collaboration on work items, yet it is impractical to propose it when collaborating with your third party business vendors for whom the cost of deployment is too high or not suited.

NextLabs Rights Management Server allows you to distribute confidential information with your business vendors who's computer network systems exist independently outside of your own network. It safeguards data privacy and integrity while permitting access to authorized personnel from your business vendors.

You can also use Rights Management Server to access your NXL protected documents while outside of your company's intranet and without installing any proprietary software on your personal computer.

Abandoning the requirement for native software installation and instead providing an independent platform for authorized viewership of sensitive information broadens the scope for collaboration and affords your organization the same level of confidence in its information risk management strategy.

Some of the key benefits of NextLabs Rights Management Server include:

- Web based solution to view NXL protected documents, which does not require any proprietary software installation 
- Secure access and collaboration to confidential and sensitive information via your computer and mobile device
- Integration with cloud storage services like Dropbox, SharePoint Online, and SharePoint On-Premise. 

## RMS and RMC

NextLabs Rights Management Server can help facilitate authorized Users if they need to edit an NXL protected document. This is done by making the NextLabs Rights Management Client (RMC) available for download.

The RMC allows Users with sufficient rights to view NXL protected documents (like pdfs and office documents) in their native applications. Authorized Users

can perform (but are not limited to) actions like editing, making copies, printing, and taking screen captures.

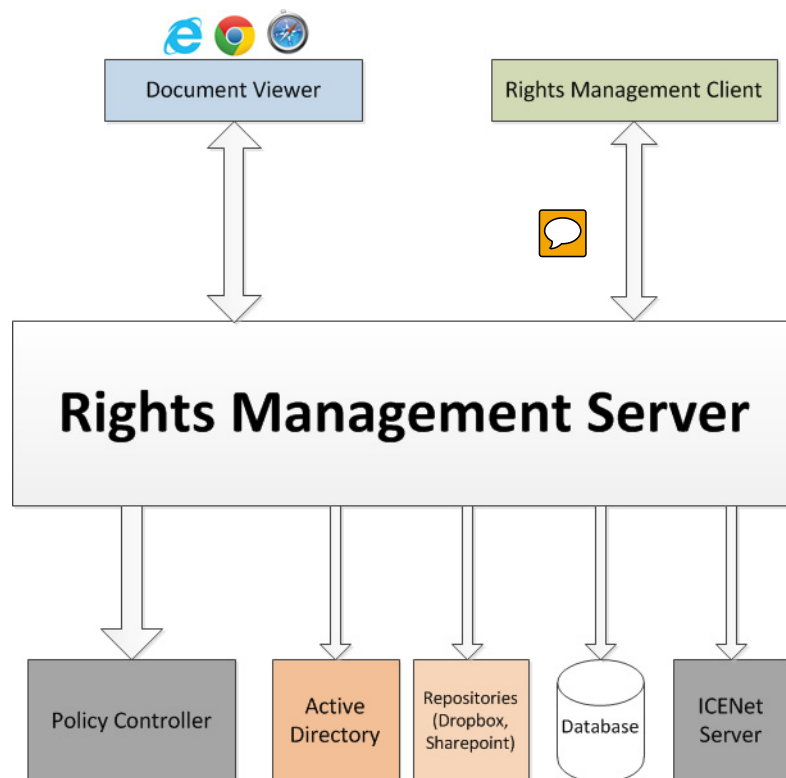
Rights Management Server communicates with the NextLabs Rights Management Client (RMC) to:

- act as an intermediary between the NextLabs Control Center and Rights Management Client
- provide the RMC with the classification tags which are used to classify documents
- ensure that all Rights Management Clients are up to date

## Logical Architecture

The following figure represents the logical architecture of Rights Management Server. The NextLabs Control Center and Java Policy Controller could reside on the same machine as the Rights Management Server or even a remote system.

The NextLabs Control Center is where you write, maintain, and deploy NextLabs Policies. The policies are sent to the Policy Controller which refers to them each time a User access request is initiated via Rights Management Server.



Rights Management Server connects to your company's Active Directory to validate users when they attempt to login to the Rights Management Server portal. Rights Management Server also connects to Microsoft SharePoint and Dropbox. This is to display a user's data.

Although Rights Management Server enables a User to view files residing in external sources, Rights Management Server only decrypts and displays NXL protected documents. Only NXL protected documents are listed in Rights Management Server. Any unencrypted files in the repository are not displayed in Rights Management Server.

Rights Management Server also allows a User to download the NextLabs Rights Management Client (RMC). Refer to the Rights Management Client documentation for details.

NextLabs protected documents are decrypted and displayed in a separate web browser window. Rights Management Server does not keep copies of decrypted files.

### **Support for NXL Protected Documents**

Rights Management Server supports files encrypted using:

- NextLabs Rights Management Client 7.5 and 7.6
- NextLabs Rights Management Client 8.x



---

### Installing Rights Management Server

This chapter describes the basic installation and setup procedures required for Rights Management Server. These procedures are broken into the following sections:

- [Before You Start](#)
- [Installing Rights Management Server](#)
- [Uninstalling Rights Management Server](#)
- [Upgrading Rights Management Server from 8.0/8.1 to 8.3](#)
- [Starting/Stopping/Restarting RMS Service](#)

### Before You Start

Before you start installing and configuring Rights Management Server, note the following requirements.

#### Prerequisites

##### Supported Platforms

- MS Windows Server 2008 R2
- MS Windows Server 2012 R2
- RHEL 6.5 and 7.1

*Note:* Among all the CAD file formats, only the SAP (VDS and RH) file formats are supported by RHEL.

- CentOS 6.0 and 7.0

##### NextLabs Software

The following must be installed before you can begin installing Rights Management Server:

- NextLabs Control Center version 7.7
- NextLabs Policy Studio, version 7.7 (or any version compatible with NextLabs Control Center)

##### Supported Databases

RMS requires a database running on its own dedicated server to store all system data. The current release supports the following databases:

- Oracle
- MS SQL Server
- MySQL

Each of these options involves different requirements on the database side, which should be taken care of before you begin RMS installation.

##### Oracle

1. Install the Oracle database software on your database server. For an existing database, the DBA must allocate sufficient space in it.
2. Create a valid username and password to access the database. This user account must be granted the CREATE VIEW or CREATE ANY VIEW system privilege. This user account must also have privileges to add and drop tables, insert and delete data, read data, and create indexes; however, it should not have a DBA role. It is recommended that you configure a user with Connect & Resource roles. You will need to provide the database user ID name and password when prompted during RMS installation.



### **MS SQL Server**

1. Install the MS SQL Server database software on your database server. For an existing database, the DBA must allocate sufficient space in it.
2. MS SQL Server must be set to mixed authentication mode.
3. Create a valid username and password to access the database. This user account has the following requirements:
  - User's default database must be the same as the database schema being used
  - User must have administrative access to the database schema
  - User must have privileges to add and drop tables, insert and delete data, read data, and create indexes
  - User must be a Local DB user
  - User must not be required to change password at first login
4. You will need to provide the database user ID name and password when prompted during RMS installation.
5. While creating database, select a case-sensitive collation based on your regional settings. Case sensitive collations have `_CS_` in their name.

### **MySQL**

1. Install the MySQL Server database software on your database server. For an existing database, the DBA must allocate sufficient space in it.
2. Use the following configuration while creating the database:
  - Default Character set: `utf8mb4` (`utf8` if `utf8mb4` is not available)
  - Default Collation: `utf8mb4_bin` (`utf8_bin` if `utf8mb4_bin` is not available)
  - Some versions of MySQL workbenches do not apply collation changes correctly. You can verify that by checking the database properties using Schema Inspector. If the default collation is not set to `utf8mb4_bin`, you can edit the same using the following command:  
`ALTER DATABASE db_name CHARACTER SET utf8mb4 COLLATE utf8mb4_bin`

### **Supported Web Browsers**

The Rights Management Server user interface is supported on the following web browsers:

- Internet Explorer (Versions 10 and 11) \*


- Chrome for Windows (Version 44.0.2403.125m and above) \*
- Mobile web browsers:
  - Android: Chrome 34.1 and above \*
  - Safari for iOS 8 \* and iOS 9

\* 3D files are only supported on IE 11, Chrome, Chrome on Android, Safari on iOS and Mac OS X. However, rh files are supported on IE 10 and 11. For rh files you must have the SAP Visual Enterprise Viewer product installed on the client(s).

*Note:* Web Graphics Library (WebGL) must be enabled on your web browser if you want it to render a 3D file. When viewing CAD files in RMS it is highly recommended that you use Chrome instead of Internet Explorer (for better performance).

## Supported File Formats

The table shows the file types supported by NextLabs Rights Management Server.

Doc Types	Extension	Comments
Microsoft Office	doc, docx, ppt, pptx, xls, xlsx, vsd	PowerPoint slides that contain Smart Art created prior to Microsoft Office 2007 Service Pack 2 are not supported.
Adobe Acrobat	pdf	
Autocad	dwg	For Windows OS, the dwg file will be displayed in a 3d viewer. For Linux, it will be displayed in a 2d viewer.
	dxf	
Text document	txt	
Images	png, jpg, tiff 	
jt and prt		The right to view Product and Manufacturing Information (PMI) is only supported for CAD files (excluding VDS files). For more details on how to configure these Rights, refer to <a href="#">Configuring Rights for Control Center</a> . Watermarks are not supported for rh files.
SAP	rh vds	
eDrawings 2015	sldprt sldasm prt	
Common	igs stp stl step	
Solid Edge	par psm asm (See the Note on page 19)	
Catia V5	cgr CATPart CATProduct (See the Note on page 19)	
Catia V6	3dxml	
Pro/Engineer & Creo	prt	
Parasolid	x_t x_b xmt_txt	
AutoCad, Inventor, TrueView	ipt iam (See the Note below)	

**Note:** Before you upload an assembly file and its sub-parts to view in RMS, perform the following steps:

1. Zip the assembly file and the sub-parts that are in the CAD nxl format.

2. Name the zip file same as the assembly file. Make sure the assembly file name is unique and is not same as its sub-parts.

*Note:* You cannot view the assembly file in **SharePoint on-premise** or **SharePoint Online** for this release. The **View in secure collaboration** menu is not enabled for the assembly file.

In this release, the unprotected files which are supported by RMS can be visualized in the RMS viewer. The unprotected files are, by default, given full viewing rights, and the rights-protected files will continue to have restricted viewing rights depending on the policy.

*Note:* In the case of CAD archives, RMS supports a combination of protected and unprotected files. If a CAD archive were to contain a single rights-protected file denying viewing rights by the policy, the entire archive would not be displayed to the user.

### Database for Location lookup

Rights Management Server queries an offline version of the third party database, WebNet77, which provides the physical location for an IP address. This query information is used by Rights Management Server to determine if the User should be granted permission for an action, based on which geographic location the user request being generated from.

*Note:* Only IPv4 addresses are supported.

Rights Management Server periodically does an auto update of the offline location database. This requires a connection to the Internet. The frequency of updates is configurable in the Settings page. You can also configure Rights Management Server to not update this location database.

By default this option is turned off. If you attempt to define policies that are based on the User's location then you need to enable this option. For more information, refer to [Configuring User Location Settings](#).

---

## Installing Rights Management Server

You can install RMS on a Windows server or a Linux server, using one of the following installation modes:

- An installation wizard that guides you step-by-step through the installation
- Silent installation, which you launch from a command prompt after supplying input values in a file

*Note:* If you are connecting to a Linux server using the command line Telnet session, you must run the silent installation. The installation wizard does not run over a Telnet session.

To install RMS, you should log in as an Administrator on a Windows OS or as a root user on a Linux OS.

## Installing Viewers

In order to view the SAP, Document, and CAD files in RMS, install the Document, CAD, and SAP viewer packages as shown below. See Uninstalling Viewers ([page 35](#)) to uninstall viewers manually.

1. Get the Document, CAD, or SAP Viewers from NextLabs support and place it under `<RMS_INSTALL_DIR>/viewers`. Do not rename the files. Keep only a single zip file, for each viewer.
2. Restart the Rights Management Server.

## License Key File

To view the RMS supported files described in the section [Supported File Formats](#), you will need the `license.dat` file. If you do not need this functionality, you can skip the step to provide the license details in the installation wizard. At any time after the installation, If you want to use this feature, you can copy the `license.dat` file to the `<RMS_DATA_DIR>/license` folder and restart the Rights Management server.

Contact NextLabs Technical Support to obtain the license key file.

## Running the Installation Wizard

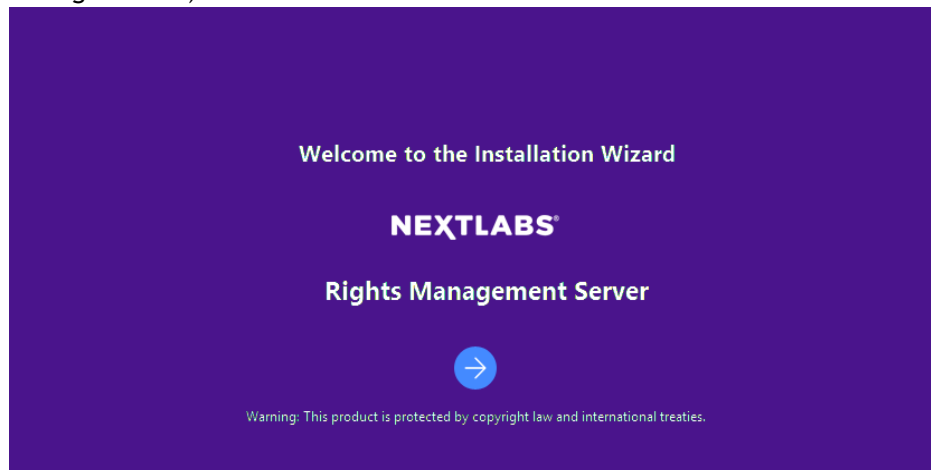
To install the server components of RMS, using the Installation Wizard, follow these steps:

1. Locate the installation zip file, provided by NextLabs support, and extract the file. The installation zip files are separate for Windows and Linux.
2. Run the installer as follows:
  - On a Windows server, you can launch the installer from one of the following methods:
    - launch the command prompt as an Administrator.

- In the command prompt, navigate to the folder that contains **install.bat**.
- From this directory, run the following command: `install.bat`

OR

- right click the **install.bat** file from the installation folder and select **Run as administrator**.
- On a Linux server
    - launch the terminal.
    - In the terminal, navigate to the folder that contains **install.sh**.
    - From this directory, run the following command as root:  
`./install.sh`
3. On the Welcome screen of the RMS Installation Wizard, click **Next** (the right arrow).



4. On the License Agreement screen, click **Agree and Proceed**.
5. Select the components to be installed on the machine:
  - Rights Management Server (RMS) - Enables users to view rights protected and unprotected files residing in an external repository through RMS or from RMS.
  - Key Management Server (KMS) -The Key Management Server allows administrators to create shared keys and send them to endpoints. The Key Management Server can be installed on the same machine as Rights Management Server or on a different server.
6. Specify the location of the **license.dat** file and click **Next**. You need the license file to view a file in RMS. If you do not have a license, you can skip

this step and add later as described in the section License Key File (page 21).

**NEXTLABS®** Rights Management Server

**License File Location**

Please specify the license file required for viewing CAD files in Rights Management Server. If you have not obtained this file, you can skip this step for the moment and contact NextLabs to request for a license file.

**Browse**

← Back Cancel Next →

- Specify the folders to install RMS and save RMS data. You can accept the default folders, and click **Next**. If the folders do not exist, the installer will prompt whether you want to create a new folder.

*Note:* It is recommended to use the default values for these settings.

**NEXTLABS®** Rights Management Server

**Installation/Data Directories**

Please specify the installation and data directories where Rights Management Server will be installed.

Install Rights Management Server to:

**Browse**

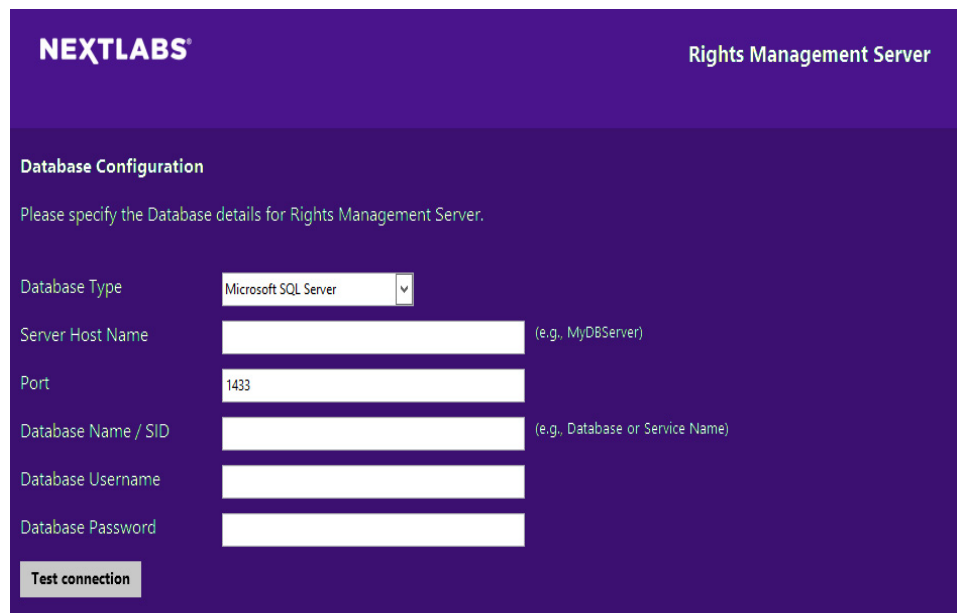
Save Rights Management Server data to:

**Browse**

← Back Cancel Next →

- Accept the default communication ports or change them, and click Next. As a rule, you should accept the default port numbers, unless you know they are already (or will be) in use by some other process in your system.

- **SSL port number:** Enter the port number to access RMS using HTTPS. The default port number is 8443.
  - **Shutdown port number:** Enter the shut down port that will be used by RMS. The default port number is 8005.
9. Choose the database where RMS stores the repository settings and other data. You may specify the database type as In-Built or one of external databases like MySQL, Oracle, Microsoft SQL server. If you select an external database, specify the database connection information such as the host name, port, database name, user name, password. If you select an In-Built database, enter the port number and the database password. Select **Reuse these settings for KMS database configuration** to reuse the RMS database settings for KMS database configuration. Click **Test Connection** to test if the connection is successful. After the connection is successful, click **Next**.



The screenshot shows the 'Database Configuration' screen of the NextLabs Rights Management Server. The header includes the 'NEXTLABS' logo and 'Rights Management Server'. Below the title, a message says 'Please specify the Database details for Rights Management Server.' The form contains several input fields: 'Database Type' (a dropdown menu currently showing 'Microsoft SQL Server'), 'Server Host Name' (with a placeholder '(e.g., MyDBServer)'), 'Port' (with the value '1433'), 'Database Name / SID' (with a placeholder '(e.g., Database or Service Name)'), 'Database Username', and 'Database Password'. At the bottom left of the form is a 'Test connection' button.

10. Configure the Active Directory or OpenLDAP. NextLabs Rights Management Server integrates with Microsoft Active Directory (AD) or OpenLDAP and uses it to authorize users.
- **LDAP Type** - Select **OpenLDAP** or **Active Directory**.
  - **Server Host Name** - The name of your AD/OpenLDAP server. For example, MyADServerName.
  - **Domain Name** - The name of the domain your AD/OpenLDAP server is on. For example, mydomain.companydomain.com
  - **Search Base** - The location in your AD/OpenLDAP where you want to begin validating user credentials. For example: DC=mydomain, DC=companydomain, DC=com



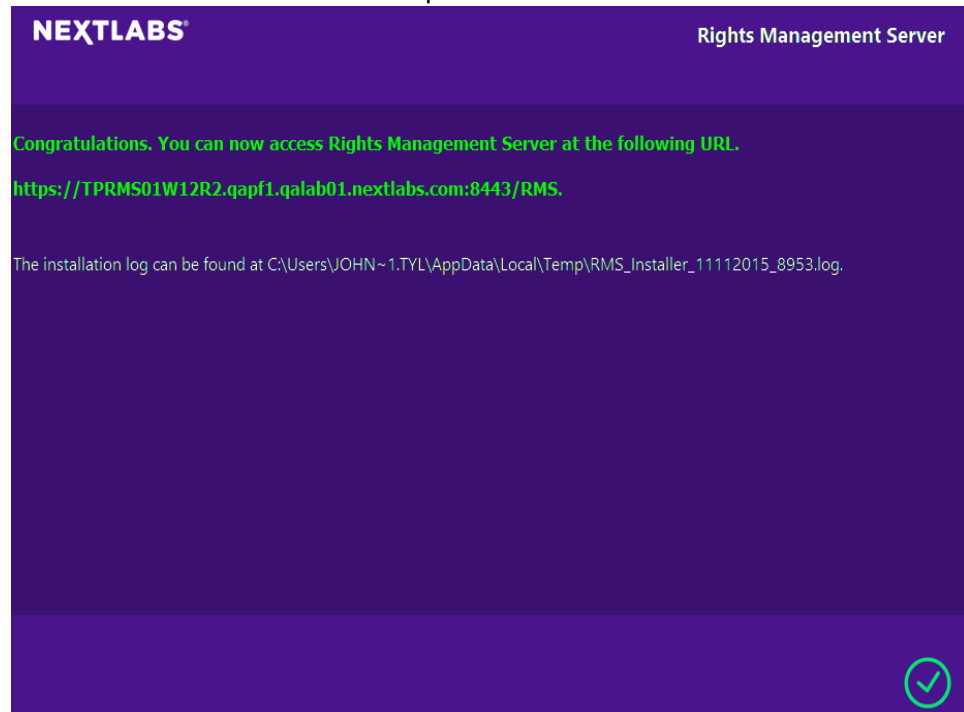
- **User Group** - The name of the User Group whose members are allowed to login. This field is optional. If not specified, all users in the AD/OpenLDAP will be allowed to access RMS.
- **RMS Administrator** - The name of the Rights Management Server Administrator account.  
**NOTE:** The Administrator must belong to the User Group if specified.

11. Enter the **RMI port for Key Management**. RMS communicates with the Embedded Java Policy Controller for key management via RMI. Specify the port number to be used for this communication. The default port number is 1099.
12. Enter the IP Address or the fully qualified domain name (FQDN) of the ICENet Server in the following format: **https://<ICENet-server-name>:<portnumber>**. For example: **https://myICENetServer:9191**.

To modify the ICENet Server address after the installation, perform the following steps:

- Go to **<RMS\_DATA\_DIR>\javapc\config\commprofile.xml**, and update the **DABSLocation** field.
  - Update the ICENet Server URL in the RMS web portal. Refer to the section [Configuring Client Management Settings \(page 55\)](#) for details.
13. Enter the keystore password.
  14. Click **Next** to begin installation. You will receive a notification when the installation is complete.

15. Click **Next**. If the installation is successful, you will see the following screen as shown in the example below.



If the installation is not successful, the installer will roll back the installation to the older version.

16. After the installation, configure the minimum and maximum memory sizes of the Rights Management Server. It is recommended to set a value of at least 1024 MB for the Maximum memory pool. Refer to the section [Configuring RMS Memory Settings \(page 68\)](#) for details on how to increase the memory size.

### Running a Silent Installation

To install the server components of RMS using the silent installation mode, follow these steps:

1. Locate the installation zip file, provided by NextLabs support, and extract it.
2. Edit the **setup.json** file to supply installation values. This file is located in the installation directory where the **install** script is present. You can edit the json file using a text editor. The file contains the following fields:
  - **installation\_dir** - This field is not applicable for Linux. RMS will use the default path for Linux. For Windows, you may specify the folder to install RMS, it is optional. Make sure you use the forward slash and not the backward slash to define the installation directory path.

The default path for

- **Windows** - C:/Program Files/NextLabs/RMS
  - **Linux** - /opt/nextlabs/RMS
- **data\_dir** - This field is not applicable for Linux. RMS will use the default path for Linux. For Windows, you may specify the folder path to install RMS data, it is optional. It is recommended not to set a new directory path unless necessary. Make sure to use the forward slash and not the backward slash to define the data directory path.

The default path for

- **Windows** - C:/ProgramData/NextLabs/RMS/datafiles
  - **Linux** - /var/opt/nextlabs/RMS/datafiles
- **rms\_ssl\_port** - Enter the port number to access RMS using HTTPS. The default value is 8443.
  - **rms\_shutdown\_port** - Enter the port number to shut down RMS. The default port number is 8005.
  - **rmi\_km\_port** - Enter the port number to communicate with the Embedded Java Policy Controller for key management. The default port is 1099.
  - **icenet\_server** - Enter the IP Address or the fully qualified domain name (FQDN) of the ICENet Server in the following format:  
`https://<ICENet-server-name>:<portnumber>`  
For example: `https://myICENetServer:9191`

To modify the ICENet Server address after the installation, go to `<RMS_DATA_DIR>\javapc\config\commprofile.xml`, and update the `DABSLocation` field.

- **license\_file\_location** - Specify the location of the `license.dat` file in order to view the supported files. You can leave this field empty if you do not have the `license.dat` file at the time of installation.
- **AD Configurations** - Configure the Active Directory or OpenLDAP. Rights Management Server integrates with Microsoft Active Directory (AD) or OpenLDAP and uses it to authorize users.
  - **ldap\_host\_name** - Enter **AD** or **OpenLDAP**.
  - **ldap\_domain** - Enter the name of the domain your AD/OpenLDAP server is on. For example, `mydomain.companydomain.com`.
  - **ldap\_search\_base** - Enter the location in your AD/OpenLDAP where you want to begin validating user credentials. For example: `DC=mydomain, DC=companydomain, DC=com` RMS communicates with the Embedded Java Policy Controller for key management via RMI. Specify the port number to be used for this communication.
  - **ldap\_user\_group** - Enter the name of the User Group who's members are allowed to login.

- **ldap\_admin** - Enter the name of the Rights Management Server administrator account.
- Components to install:
  - **component\_rms** - If the value is set to yes, RMS will be installed. The default value is yes.
  - **component\_kms** - If the value is set to yes, KMS will be installed. The default value is yes.
- Options for RMS component:
  - **km\_server** - [Optional] The URL for standalone Key Management Server. The default value is "https://[rms\_hostname]:[rms\_ssl\_port]"
  - **rms\_db\_type** - Supported databases are **MSSQL**, **ORACLE**, **MYSQL**, **IN\_BUILT**. The **IN\_BUILT** database is integrated with the application without requiring any additional configuration.
  - **rms\_db\_host\_name** - Enter the database host name for all database types except **IN\_BUILT** database.
  - **rms\_db\_port** - Enter the port number for all database types.
  - **rms\_db\_name** - Enter the database name for all database types except **IN\_BUILT** database.
  - **rms\_db\_username** - Enter the database user name for all database types except **IN\_BUILT** database. For **IN\_BUILT** database type, the user name is root.
  - **rms\_db\_password** - Enter the password for all database types. This step is optional except for the **IN\_BUILT** database.
  - **rms\_db\_conn\_url** - [Optional] Specify the database connection URL. If this value is specified, it ignores **rms\_db\_host\_name**, **rms\_db\_port** and **rms\_db\_name** attributes.
- Options for KMS Component:
  - **km\_keystore\_password** - Enter the password for Keystore in KMS (min. six characters).
  - **kms\_db\_type** - Supported databases are **MSSQL**, **ORACLE**, **MYSQL**, **IN\_BUILT**.
  - **kms\_db\_host\_name** - Enter the database host name for all database types except **IN\_BUILT** database.
  - **kms\_db\_port** - Enter the port number for all database types.
  - **kms\_db\_name** - Enter the database name for all database types except **IN\_BUILT** database.
  - **kms\_db\_username** - Enter the database user name for all database types except **IN\_BUILT** database. For **IN\_BUILT** database type, the user name is root.
  - **kms\_db\_password** - Enter the password for all database types. This step is optional except for **IN\_BUILT** database.

- kms\_db\_conn\_url - [Optional] Specify the database connection URL. If this value is specified, it ignores kms\_db\_host\_name, kms\_db\_port and kms\_db\_name attributes.
3. Run the installer as follows:
    - On a Windows server
      - launch the command prompt as Administrator.
      - In the command prompt, navigate to the extracted folder.
      - From this directory, type the following command to run the installer in the silent mode: `install.bat -s`
    - On a Linux server
      - navigate to the extracted folder.
      - From this directory, type the following command to run the installer in the silent mode: `./install.sh -s`
  4. The installation logs can be found in the following locations:
    - On a Windows server
      - %temp%/RMS\_Installer\_<Timestamp>.log
    - On a Linux server
      - /tmp/RMS\_Installer\_<TimeStamp>.log
  5. After the installation, configure the minimum and maximum memory sizes of the Rights Management Server. It is recommended to set a value of at least 1024 MB for the Maximum memory pool. Refer to the section [Configuring RMS Memory Settings \(page 68\)](#) for details on how to increase the memory size.

## Logging in to the Rights Management Server Portal

1. Type the following URL in your web browser:
 

**https://<Your Rights Management Server hostname or IP Address>:<https port number>/RMS**

*Note:* For example, `https://mysecurecollaborationserver:8443/RMS`
2. Type your Username, Password, and select the domain to which your Rights Management Server is connected.
3. Click **Log in**.

## Minimum Screen Resolution

The Rights Management Server console is best viewed at a minimum screen resolution of 1366 x 768.

*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.

### Accessing Rights Management Server using Internet Explorer

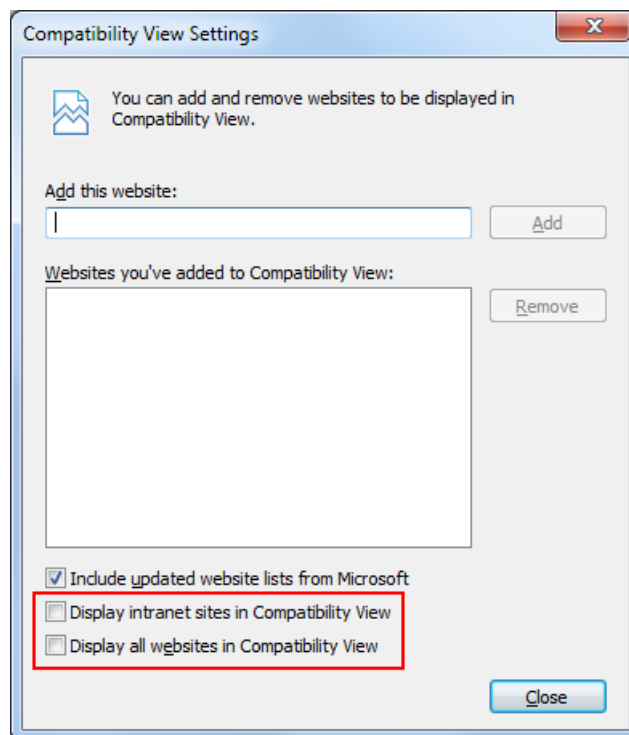
The following options must be configured before you use Internet Explorer (IE) to access Rights Management Server.

#### ***Compatibility View Settings***

If you are using Internet Explorer (IE9 or IE10) to access the Rights Management Server user interface then you must switch off the compatibility view.

The compatibility view is meant for accessing web pages that have been designed for earlier version of Internet Explorer. Attempting to view Rights Management Server in Internet Explorer with compatibility view switched on renders the UI in an inconsistent manner.

1. In Internet Explorer, navigate to **Tools > Compatibility View settings** in the menu bar.
2. Un-check the following options:

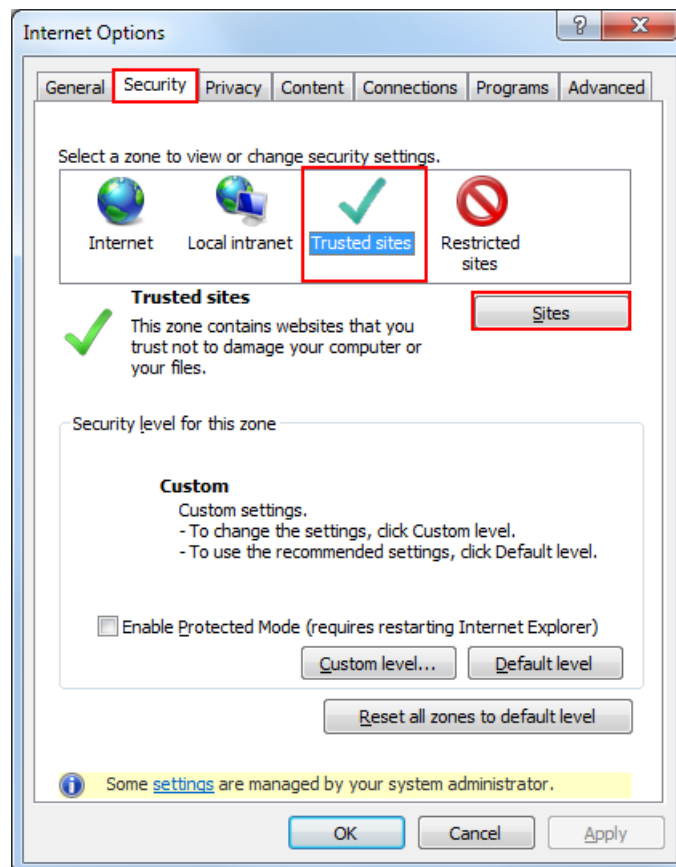


- Display Intranet sites in Compatibility View
- Display all websites in Compatibility View

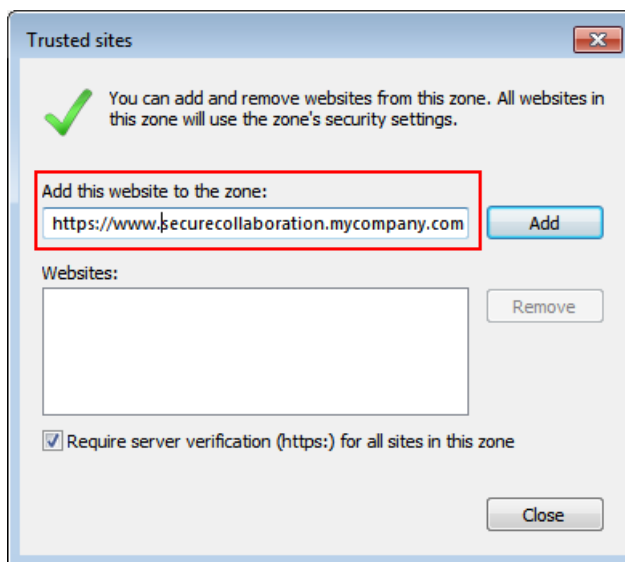
### Trusted Sites

You must also add the URL of your Rights Management Server portal as a Trusted Site in Internet Explorer. This allows JavaScript execution when you access the Rights Management Server portal.

1. In Internet Explorer, navigate to **Tools > Internet Options** in the menu bar.
2. Click the **Security** tab and select **Trusted Sites**.
3. Click **Sites**.



4. In the Trusted Sites window, type the URL of your Rights Management Server portal and click **Add**.



5. Click **Close**.
6. In the Internet Options window, click **OK**.



## Uninstalling Rights Management Server

You can uninstall RMS on a Windows server or a Linux server, using one of the following modes:

- An uninstallation wizard that guides you step-by-step through the uninstallation.
- Silent uninstallation, which you launch from a command prompt after supplying input values in a file.
- On a Windows server
  - launch the command prompt as an Administrator.
  - In the command prompt, navigate to the `<RMS_INSTALL_DIR>` directory that contains **uninstall.bat**.
  - From this directory, run the following command: `uninstall.bat` and follow the instructions.

OR

- right click the **uninstall.bat** file from the installation folder and select **Run as administrator**.
- On a Linux server
  - launch the terminal.
  - In the terminal, navigate to the `<RMS_INSTALL_DIR>` directory that contains **uninstall.sh**.
  - From this directory, run the following command as root: `./uninstall.sh` and follow the instructions.

## Performing a silent Uninstallation

To uninstall the RMS server components using the silent mode, follow these steps:

1. Edit the **setup.json** file in `<RMS_INSTALL_DIR>/uninst` to supply uninstallation values. You can edit the json file using a text editor.
2. Update the **delete\_data\_dir** field to **Yes** if you want the uninstaller to delete the data directory which contains log files and configuration files. The default value is **No**. The installation directory will always be deleted during uninstallation.
3. Run the uninstaller as follows:
  - On a Windows server
    - launch the command prompt as Administrator.
    - In the command prompt, navigate to the `<RMS_INSTALL_DIR>`.

- From this directory, type the following command to run the uninstaller in the silent mode: `uninstall.bat -s`
- On a Linux server
  - navigate to the `<RMS_INSTALL_DIR>`.
  - From this directory, type the following command to run the uninstaller in the silent mode: `./uninstall.sh -s`

---

## Uninstalling Viewers

Perform the following steps to uninstall Document, CAD, or SAP viewers manually.

### Uninstalling Document Viewer

1. Stop the Rights Management Server. See Starting/Stopping/Restarting RMS Service ([page 37](#)) for details.
2. Delete the viewer package from <RMS\_INSTALL\_DIR>/viewers.
3. Delete the **perceptive** folder from <RMS\_INSTALL\_DIR>/external/perceptive.
4. Delete the **RMS** folder from <RMS\_INSTALL\_DIR>/external/tomcat/webapps.
5. Restart the Rights Management Server.

### Uninstalling CAD Viewer

1. Stop the Rights Management Server. See Starting/Stopping/Restarting RMS Service ([page 37](#)) for details.
2. Delete the viewer package from <RMS\_INSTALL\_DIR>/viewers.
3. Delete the **perceptive** folder from <RMS\_INSTALL\_DIR>/external/RMSCADCONVERTER.
4. Delete the **RMS** folder from <RMS\_INSTALL\_DIR>/external/tomcat/webapps.
5. Restart the Rights Management Server.

### Uninstalling SAP Viewer

1. Stop the Rights Management Server. See Starting/Stopping/Restarting RMS Service ([page 37](#)) for details.
2. Delete the viewer package from <RMS\_INSTALL\_DIR>/viewers.
3. Delete the **RMS** folder from <RMS\_INSTALL\_DIR>/external/tomcat/webapps.
4. Restart the Rights Management Server.

---

## Upgrading Rights Management Server from 8.0/ 8.1 to 8.3

If there is a RMS 8.0 or 8.1 version installed, you can run the **install.bat** file to upgrade it to the new version without uninstalling the existing version. Follow the steps described in the section, Running the Installation Wizard ([page 21](#)) for details.

Before you begin to upgrade, take note of the following tasks:

- Stop the Tomcat server where the RMS 8.0/8.1 version is deployed.
- Remove the following values if present from the system path:
  - For Linux: Remove the path <tomcat\_home\_dir>/webapps/RMS/WEB-INF/lib/linux/intel-64/fonts from the LD\_LIBRARY\_PATH and remove the ISYS\_FONTS environment variable.
  - For Windows: Remove the path <tomcat\_home\_dir>\webapps\RMS\WEB-INF\lib\windows\intel-64 from the PATH variable.
- To view the RMS [Supported File Formats](#), you will need the license.dat file. If you do not need this functionality, you can skip the step to provide the license file path in the installation wizard. At any time after the installation, If you want to use this feature, copy the license.dat file to the <RMS\_DATA\_DIR>/license folder and restart the Rights Management Server.
- When you are configuring the path for the RMS data directory in the installation wizard, make sure the data directory path is same as the older version.
- While configuring the Active Directory settings in the installation wizard, the installer will read the existing settings defined in the data directory. Verify that the AD settings are same as the older version.
- Refer to the Configuring Rights Management Server ([page 39](#)) chapter for steps to configure the Tomcat memory sizes and importing the existing Tomcat SSL certificates from the certified authorities.

---

## Starting/ Stopping/ Restarting RMS Service

After the RMS installation, the **NextLabs Rights Management Server** service will start automatically. If the service fails and you need to restart it, you can do so by restarting the RMS service. As with any Windows service, you must have the local administrator privileges to do this.

On a Windows machine, open the **Services** window using the **Control Panel > System and Security > Administrative Tools** menu.

- To restart the RMS service, right click **NextLabs Rights Management Server** and select **Restart**.
- To stop the service, right click **NextLabs Rights Management Server** and select **Stop**.
- To start the service, right click **NextLabs Rights Management Server** and select **Start**.

To start/stop/restart the RMS service on a Linux server, use the following commands as a root user:

- **rms restart** to restart the RMS service.
- **rms start** to start the RMS service.
- **rms stop** to stop the RMS service.



### Configuring Rights Management Server

This chapter describes configuration steps for NextLabs Rights Management Server. Note that your configuration will be specific to your product implementation.

*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.

Configuration procedures are broken into the following sections:

- [Configuring your Java Policy Controller](#)
- [Configuring a NXL Filter for MS SharePoint](#)
- [Configuring Alternate Access Mapping](#)
- [Configuring Logging](#)
- [Configuring the Remote Policy Controller Settings](#)
- [Configuring the Mail Server Settings](#)
- [Configuring Client Management Settings](#)
- [Configuring User Location Settings](#)
- [Other Configuration Parameters](#)
- [Configuring Watermark Information](#)
- [Configuring Rights for Control Center](#)
- [Configuring Rights Management Obligation](#)
- [Configuring the Rights Management Client](#)
- [Configuring RMS Memory Settings](#)
- [Importing Your Own SSL Certificates for Rights Management Server](#)

---

## Configuring your Java Policy Controller

*Note:* By default, RMS comes packaged with an embedded Java Policy Controller. If needed, you can configure RMS to communicate with an external Java Policy Controller. To configure an external Java Policy Controller, follow the steps mentioned below.

Before you begin configuring your Rights Management Server-Java Policy Controller communication, you must verify that the following software components must be installed for your Java Policy Controller:

- Java SDK
- Key Management Service

For more information, refer to the *Control Center Installation Guide*.

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.

*Note:* If you do not intend to use the Document Viewer in your Rights Management Server deployment then you do not need to specify this information.



## Configuring Remote Java Policy Controller Communication

The Java Policy Controller is responsible for policy evaluation and providing the encryption keys that are used by the Rights Management Server to decrypt files. In order to establish secure communication between these two components KeyStore and TrustStore files must be configured for both components.

The following sections detail the configuration process for both components (Rights Management Server and the Java Policy Controller).

*Note:* Generating the KeyStore file, exporting the file as a certificate, and importing the file as a TrustStore are steps that typically should be done for Rights Management Server-Java PC and Java PC-Rights Management Server communication separately. The following sections detail steps to create a KeyStore certificate and add it to the Rights Management Server TrustStore for Rights Management Server-Java PC communication. You can use the same files for Java PC-Rights Management Server communication as well, i.e. you can add the same Certificate to the Rights Management Server TrustStore. Or you can create a new Certificate for the Java-PC and import it into the Rights Management Server TrustStore.

If you want to avoid some of the steps listed below ([Generating the Certificate](#), [Exporting the Certificate](#), and [Importing the Certificate into the TrustStore](#)), then you can instead use the default KeyStore files which are included with the installation package and can be used for your deployment. The files are located at the following location:

`<RMS_DATA_DIR>/cert`

The files included are:

- `rmskmc-keystore.jks`
- `rmskmc-truststore.jks`

The encrypted password for these keystore files is:

`sa1f78f49e437288039751654ece96ede`

The unencrypted password for these keystore files is `123next!`.

Using these files and information you can continue to the [Adding Attributes to the KeyManagement Services File](#) section.

### KeyStore & TrustStore Files

The Java Policy Controller is responsible for policy evaluation and providing the encryption keys that are used by the Rights Management Server to decrypt files. In order to establish secure communication between these two components KeyStore and TrustStore files must be configured for both components.

Generating the KeyStore file, exporting the file as a certificate, and importing the file as a TrustStore are steps that typically should be done for Rights Management Server-Java PC and Java PC-Rights Management Server communication separately.

The following sections detail steps to create a KeyStore certificate and add it to the Rights Management Server TrustStore for Rights Management Server-Java PC communication.

You can use the same files for Java PC-Rights Management Server communication as well, i.e. you can add the same Certificate to the Rights Management Server TrustStore, or you can create a new Certificate for the Java-PC and import it into the Rights Management Server TrustStore.

The following sections detail the configuration process for both components (Rights Management Server and the Java Policy Controller).

**Note:** For the sake of convenience KeyStore (`rmskmc-keystore.jks`) and TrustStore (`rmskmc-truststore.jks`) files have been included at the following location: `<RMS_DATA_DIR>/cert`. You can use these files if you do not want to create your own set of files as listed below. The password for both these files is `123next!`

### Generating the Certificate

1. In Rights Management Server, open your command prompt as the Administrator and type the following command, then press <Enter>:

```
keytool -genkey -alias <aliasname> -keyalg RSA -keystore  
<keystore-file-withpath>
```

where `aliasname` and `keystore` file name can be any string. An example would be:

```
keytool -genkey -alias rmskmc -keyalg RSA -keystore  
C:\temp\rmskmc-keystore.jks
```

2. Type and confirm the KeyStore password.
3. Type your full name.
4. Type your Organizational Unit (OU) name.
5. Type the name of your City or Locality.
6. Type the name of your State or Province.
7. Type the two digit country code for your State or Province.
8. Type yes to confirm your information.
9. Type the key password for your KeyStore file.

*Note:* Press <Enter> if this password is the same as the KeyStore password.

### Exporting the Certificate

1. In your Rights Management Server Server, open your command prompt as the Administrator and type the following command, then press <Enter>:

```
keytool -export -alias <aliasname> -keystore <keystore-  
file-withpath> -rfc -file <certificate-file-with-path>
```

where `aliasname`, `keystore`, and `certificate` file names can be any string. An example would be:

```
keytool -export -alias rmskmc -keystore C:\temp\rmskmc-  
keystore.jks -rfc -file C:\temp\rmskmc.cer
```

2. Type the KeyStore password.

### Importing the Certificate into the TrustStore

1. Copy the KeyStore file and Certificate to your Java Policy Controller.
2. In your Java Policy Controller machine, open your command prompt as the Administrator and type the following command, then press <Enter>:

```
keytool -import -alias <aliasname> - file  
<Certificatefile-with-path> -keystore <truststorefile-  
with-path> -storepass <password>
```

where `aliasname`, `certificate`, and `truststore` file names can be any string. An example would be:

```
keytool -import -alias kmcca -file C:\JavaPC\rmskmc.cer -  
keystore C:\MyJavaPC\mytruststore.jks -storepass  
safestorepwd32
```

3. Review your certificate details and type Yes, then press <Enter> add this certificate to your TrustStore.

### Adding Attributes to the KeyManagement Services File

1. In the Java Policy Controller, navigate to the `KeyManagementService.properties` file.
2. Add attributes in the following format to the `KeyManagementService.properties` file:

```
truststore=<truststore-filepath>  
  
keystore=<keystore-filepath>  
  
trustpass=<encrypted truststore password>  
  
keypass=<encrypted keystore password>
```

For example:

```
truststore=C:/apache-tomcat-6.0.37/nextlabs/dpc/
jservice/KeyManagement/jar/rmskmc-truststore.jks

keystore=C:/apache-tomcat-6.0.37/nextlabs/dpc/jservice/
KeyManagement/jar/rmskmc-keystore.jks

trustpass=salf78f49e437288039751654ece96ede

keypass=salf78f49e437288039751654ece96ede
```

**Note:** The trustpass and keypass are encrypted using the standard NextLabs reversible encryption tool (located in the NextLabs Control Center server, in the tools/crypt directory). For example the following command:

```
C:\Program Files\NextLabs\Policy
Server\tools\crypt>mkpassword.bat -w 123next! -e
```

results in the following keypass value:

```
salf78f49e437288039751654ece96ede
```

3. Restart your Java Policy Controller.
4. In the Rights Management Server, click **Configuration**.
5. In **POLICY CONTROLLER**, specify the **KeyStore File** and **TrustStore File** locations and passwords in the following fields:

Rights Management Server Settings Field	Description
<b>KeyStore file</b>	complete file path for the KeyStore file. This file has the certificate that is used to identify Rights Management Server to the Policy Controller. <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.
<b>KeyStore Password</b>	password for the KeyStore <b>NOTE:</b> Specify the plain text (unencrypted) passwords in Rights Management Server.
<b>TrustStore File</b>	complete file path for the TrustStore file. This file includes the certificates that are trusted by Rights Management Server.
<b>TrustStore Password</b>	password for the TrustStore <b>NOTE:</b> Specify the plain text (unencrypted) passwords in Rights Management Server.

6. Click **Save**. You do not need to restart Rights Management Server for these changes to take effect.

## Configuring a NXL Filter for MS SharePoint

If you have added a Microsoft SharePoint portal as a repository in Rights Management Server, then this involves Rights Management Server querying your SharePoint portal for NXL files.

You must specify NXL files as a file type that must be included in Microsoft SharePoint crawls. A SharePoint crawl indexes different file types and allows for (included) file types to be considered during search queries.

After specifying NXL file types in the list of file types to index for your SharePoint deployment, you must run a full crawl. This is to ensure that any NXL files that were uploaded prior to this configuration are also indexed. A partial crawl only covers NXL files uploaded after you have performed this configuration.

### Specifying the NXL File Type

1. In your SharePoint machine, open the Central Administrator screen.
2. Navigate to **Application Management > Manage Services Application > Search Service Application > File Types**.
3. Click **New File Type**.
4. Type **nxl** and click **OK**.

### Specifying NXL Registry Entries

1. In your SharePoint machine, open the Registry Editor.
2. Navigate to the following registry location:  
`HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office  
Server\<your SharePoint  
version>\Search\Setup\Filters\ .nxl`

**Note:** If this registry location is not listed then you must create it. Your SharePoint version number is based on which MS-SharePoint version you are using. For instance if you are using MS-SharePoint 2010 then the version number to specify is 14.0. For MS-SharePoint 2013 the version number to specify is 15.0.

3. Verify that the registry values are set as indicated below (if you are creating this registry location then set the following registry values):

Name	Type	Data
Default	REG_SZ	<value not set>
Extension	REG_SZ	nxl
FileTypeBucket	REG_DWORD	1
MimeTypes	REG_SZ	application/nxl
ThreadingModel	REG_SZ	Both

4. Navigate to the following registry location:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Office
Server\<your SharePoint
version>\Search\Setup\ContentIndexCommon\Filters\Extens
ion\.nsl
```

5. Verify that the registry value is set as indicated below:

Name	Type	Data
Default	REG_MULTI_SZ	{38522F37-C617-4438-BA5E-77BA8B655237}

6. In your SharePoint machine, at the command prompt type the following command to stop SharePoint Search:

```
stsadm -o osearch -action stop
```

7. After the stop command has successfully executed, type the following command, to start SharePoint Search:

```
stsadm -o osearch -action start
```

8. After the start command has successfully executed, type the following command to restart IIS:

```
IISRESET
```

9. In your SharePoint Central Administrator, navigate to **Application Management > Manage Services Application > Search Service Application > Content Sources**.

10. Where applicable right-click the SharePoint site and select **Full Crawl**.

## Configuring Alternate Access Mapping

### Configuring Alternate Access Mappings in Sharepoint 2010 and 2013

If you have specified an IP address for your SharePoint repository link then you must also set up an Alternate Access Mapping on your Microsoft SharePoint, which ensure that a fully qualified domain name (FQDN) always defaults for other URLs users might enter. You do this in SharePoint by mapping a fully qualified name as the “Internal URL” for each web zone.

1. Access the SharePoint server at **Start > All Programs > Microsoft SharePoint (2010 or 2013) Products > SharePoint (2010 or 2013) Central Administration**.
2. In the System Settings area, click **Configure alternate access mappings**.

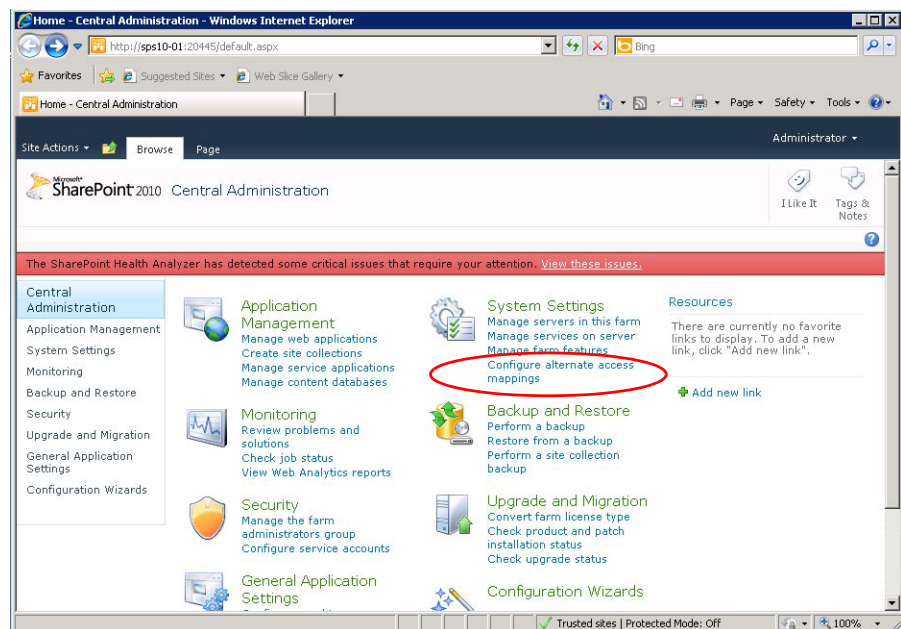


Figure 3-1: Alternate Access Mappings

3. In the Alternate Access Mappings window, click **Add Internal URLs**.

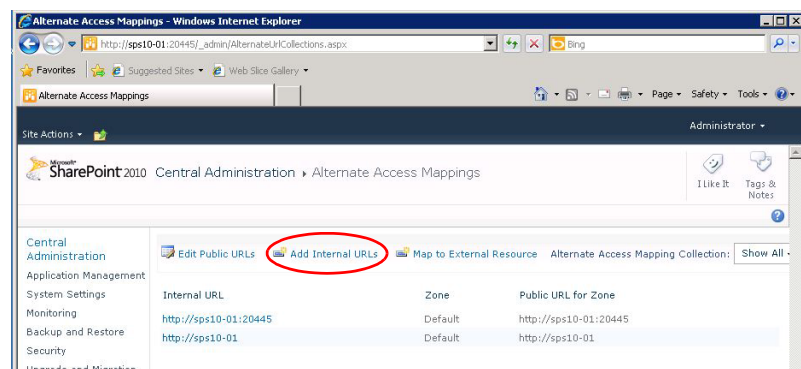
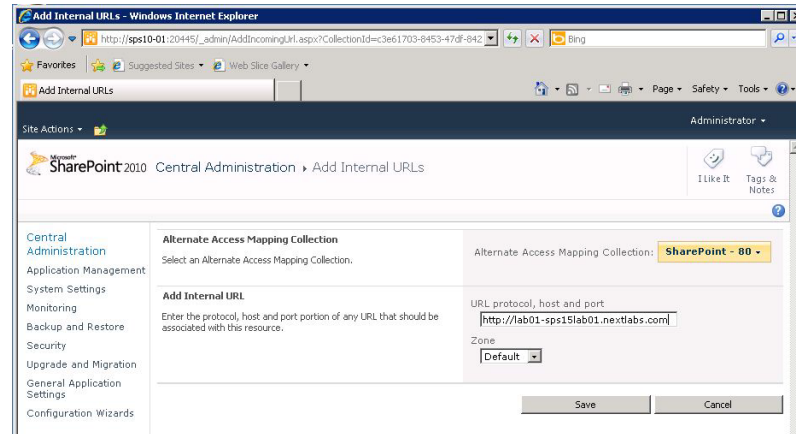


Figure 3-2: Alternate Access Mappings window

4. In the **Alternate Access Mapping Collection**, select SharePoint-80.
5. In the **URL, protocol, host and port** field, enter the fully qualified domain name of the site. In our example in the following figure, this is “http://lab01-sps15.lab01.nextlabs.com.”
6. If applicable, select the **Zone** for the URL.



7. Click **Save** to save the mapping.
8. Repeat these steps to enter a fully qualified domain name as the “Internal URL” for every configured web zone on your service. For example, you would need to do this for an “internal” zone and an “external” zone.



## Configuring Logging

The log file generated by Rights Management Server can log information at two levels (INFO and DEBUG). You can modify the Rights Management Server log properties file to toggle the level of information being written to the log file.

*Note:* You should only modify the log level (from INFO to DEBUG) if your NextLabs support person requests you do this for troubleshooting purposes. Setting the log level to DEBUG for Rights Management Server can adversely impact your server's performance. Therefore it is strongly recommended that you only make changes to this setting when requested by NextLabs support personnel and at a time when you do not anticipate your Rights Management Server to be engaged in servicing user requests.

The Rights Management Server log properties file (`RMSLog.properties`) is located at the `<RMS_DATA_DIR>`.

The log files are generated and stored at the following location:

`<RMS_DATA_DIR>\logs`

You can modify the following options in the Rights Management Server log properties file:

Log File Option	Description
<code>rootLogger</code>	this value determines the type of information logged by Rights Management Server. The default value is INFO. Set this value to DEBUG only if NextLabs Support requests you do this (for troubleshooting purpose). <b>NOTE:</b> Setting this option to DEBUG has a performance impact. Therefore plan your troubleshooting activity on the Rights Management Server accordingly. After you are done troubleshooting it is strongly recommended you set it back to INFO.
<code>MaxBackupIndex</code>	this value determines the number of files you want to create each time a log file reaches the size limit. After you hit this limit, Rights Management Server begins overwriting the log files starting from the oldest log file.
<code>MaxFileSize</code>	this value determines the size of each log file. You must specify MB with the file size, e.g. type 5MB to set a log file size of 5 megabytes.

*Note:* You do not need to restart the Web Server after making changes to the Rights Management Server log properties file.

---

## Configuring Service Providers

The RMS application provides the option to integrate with service providers such as SharePoint, Dropbox, etc in order to allow users the ability to view NextLabs rights protected files from RMS or allow users the ability to view NextLabs rights protected files directly from a service provider via RMS.

You must configure the service provider in order to grant users access to repository.

There are following three categories:

- **Configured Providers** - This section displays service providers that are integrated with Rights Management Server (RMS). This allows users to add their own personal repositories for the given service provider in RMS. If a personal repository is not configured, users can access the shared repositories.
- **Available Providers** - This section displays available service providers that RMS supports. You can configure these service providers to integrate with RMS to grant users access to the repository from RMS. After the service providers are configured, it will move to the Configured Providers. Currently, RMS supports Google Drive, OneDrive, SharePoint Online, SharePoint On Premise, and Dropbox service providers.
- **Cross-Launch Apps** - This section displays service providers that can be integrated with RMS to allow users ability to view the rights protected or unprotected files directly from the service provider. This feature is supported only by SharePoint On Premise and SharePoint Online apps.

Refer to the following sections for configuring different service providers:

- See Integrating with Google Drive ([page 101](#)) for configuring Google Drive.
- See Integrating with SharePoint Online ([page 79](#)) for configuring SharePoint Online.
- See Integrating with Microsoft OneDrive ([page 107](#)) for configuring Microsoft OneDrive.
- See Integrating with Dropbox ([page 95](#)) for configuring Microsoft Dropbox.
- See Integrating with SharePoint On-Premise ([page 85](#)) for SharePoint On Premises.

## Configuring the Remote Policy Controller Settings

Rights Management Server interacts with the Policy Controller to verify if a user is authorized to view an encrypted file.

You must specify the connection details for your Policy Controller in Rights Management Server in order to ensure that each user access request is handled appropriately based on policies that you have defined in the NextLabs Control Center.

*Note:* If you do not intend to use the Document Viewer in your Rights Management Server deployment, then you do not need to configure this information.

1. Log in to the Rights Management Server portal.
2. Click **Configuration**.
3. In the **POLICY CONTROLLER** section, enter the following details:

Field	Description
Enable Remote Policy Controller	By default, RMS comes packaged with an embedded Java Policy Controller. But if needed, you can configure RMS to communicate with an external Java Policy Controller. To configure an external Java Policy Controller, enable remote policy controller. The default value is <b>No</b> . If the remote Java Policy Controller is enabled then the fields below will be shown.
Policy Controller Hostname (Key Management)	Hostname of the machine your Policy Controller's Key Management and Policy Evaluation component is installed on. This must be specified in the following format: <code>https://&lt;server name&gt;:&lt;port number&gt;</code> For example: <code>https://RightsManagement.mycompany.com:8443</code> <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.
RMI Port Number for Key Management	The port number on which Rights Management Server communicates with the Policy Controller for the purpose of Key Management.
KeyStore file	Complete file path for the KeyStore file. This file has the certificate that is used to identify Rights Management Server to the Policy Controller. <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.
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

4. Click **TEST CONNECTION** to verify that Rights Management Server can connect to the Policy Controller.
5. Click **SAVE**.

## Configuring the Mail Server Settings

In order to collaborate with external business partners on documents, Rights Management Server has the option to facilitate user account creation for accessing the Rights Management Server portal.

When an external business partner clicks the **Request an account** option on the Rights Management Server login page, this triggers a Rights Management Server request to a SMTP mail server to send a user account creation request email to the Administrator and the sponsor.

Rights Management Server needs to communicate with an SMTP mail server to transmit emails for new user accounts to the Administrator and sponsor. These SMTP details must be configured using the Rights Management Server web portal.

1. Login to the Rights Management Server web portal.
2. Click **Configuration**.
3. In the **MAIL SERVER** section, enable **Allow Registration Request**.

*Note:* If this option is not enabled, then the **Sign Up** option is not available on the Rights Management Server login page and external users cannot request for a new user account to be created for access to the Rights Management Server web portal.

4. Enter the following details:

Field	Description
<b>Allow Registration Request</b>	This is the option to allow new account requests via the Rights Management Server login page. Setting this value to No removes the <b>Request an account</b> hyperlink from the login page.
<b>SMTP Host</b>	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.
<b>SMTP Port</b>	This is the port number at which Rights Management Server and SMTP communication occurs.
<b>SMTP Authentication needed?</b>	If you want to enable SMTP authentication prior to any email being sent due to Rights Management Server, then enable this option.
<b>SMTP User Name</b>	This is the user name for the mail account which will send emails to the Administrator and sponsor on behalf of Rights Management Server.
<b>SMTP Password</b>	This is the password for the SMTP User Name
<b>Enable TLS?</b>	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, enable this option.

Field	Description
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.

5. Click **SAVE**.

## Configuring Client Management Settings

Rights Management Server (RMS) communicates with the ICENet server to gather configuration details, policies, and classification tags which are passed to the Rights Management Client (RMC).

The section below lists the steps that must be performed to ensure the RMS, Policy Controller and Control Center communication is configured correctly.

1. In the Rights Management Server web portal, click **Configuration**.
2. In the **CLIENT MANAGEMENT** section, enter the following details:

Field	Description
ICENet Server URL	This is the IP Address or the fully qualified domain name (FQDN) of the ICENet Server in the following format: https://<ICENet-server-name>:<portnumber> For example: https://myICENetServer:9191
Client Version Number	This is the version number of the latest Rights Management Client installation file. The Rights Management Client deployed on different machines checks against this <b>Client Version Number</b> to determine if a new version of the RMC installer is available for auto upgrade.
Client Package Download URL (32-bit)	This is the URL that is used to download the 32-bit version of the Rights Management Client (RMC) installer. This is the location from where the RMC downloads the new installer.
Client Package Checksum (32-bit)	This is the Checksum value which is associated with the 32-bit installation file. This value can be generated by using the appropriate Checksum tools on the new installation file.
Client Package Download URL (64-bit)	This is the URL that is used to download the 64-bit version of the Rights Management Client (RMC) installer. This is the location from where the RMC downloads the new installer.
Client Package Checksum (64-bit)	This is the Checksum value which is associated with the 64-bit installation file. This value can be generated by using the appropriate Checksum tools on the new installation file.

3. Click **SAVE**.

---

## Configuring User Location Settings

Rights Management Server (RMS) can be configured to enforce policies which restrict access to protected documents based on the requesting user's IP address or physical location. These policies are authored in NextLabs Policy Studio. For more information, refer to [Enforcing IP Address Policies](#).

In order for such policies to be enforced by RMS, you must enable the **Turn On User Location** option in the **General Settings** section of the **Application Settings** menu.

1. In the Rights Management Server web portal, click **Configuration**.
2. In the **General** section, **Session Timeout** field, enter the minimum number of minutes before your Rights Management Server web portal session is terminated
3. Enable the **Turn on User Location** option.
4. Enter the following details:

Field	Description
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 Updated Time	This displays the last time the Location database file was updated. <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. For more information about this lookup file, refer to <a href="#">Database for Location lookup</a> .
Location Update Frequency	This is the frequency of updates performed for the Location database file.

5. Click **SAVE**.



---

## Other Configuration Parameters

You can set the following parameters in `RMSConfig.properties` file in the <Rights Management Server DATA DIR>:

- `CONVERTER_IMAGE_DPI` - This parameter is used to configure the quality of the document being viewed in the viewer. The default value of this parameter is 120.

*Note:* Increasing this value will increase the amount of memory needed for processing the documents. So increase it with a consideration to your machine's resources.

- `SHAREPOINT2013_SEARCHWITHCOUNT` - This parameter is used to configure the number of files you want to search for in the SharePoint repository. The default value is true.
- `SHAREPOINT2013_SEARCHLIMITCOUNT` - This parameter is used to configure the number of files to be searched. The value for this parameter must be lower than the `MaxRowLimit` parameter in your Microsoft SharePoint Server. For more information, refer to [FAQs](#) section.

---

## Configuring Watermark Information

You can configure Rights Management Server to display a watermark on a NXL protected document. Rights Management Server does not alter your NXL protected document in anyway during this process.

*Note:* Watermarks are not supported for rh files.

There are two approaches to configuring watermarks to display on your NXL protected documents:

### Policy based Watermark

In NextLabs Policy Studio, you can specify watermarks as a custom obligation to your policy. Whenever your policy is triggered, the watermark specified in your policy's custom obligation is displayed.

The following XML code represents the watermark or security overlay (OB\_OVERLAY) custom obligation. Before you can create a policy which uses this custom obligation, you must ensure that your NextLabs Control Center's `configuration.xml` file contains this xml code in the `<Obligations></Obligations>` section:

## XML code for configuration.xml

```

.....
<Obligation>
  <DisplayName>OB_OVERLAY</DisplayName>
  <RunAt>PEP</RunAt>
  <Name>OB_OVERLAY</Name>
  <Arguments>
    <Argument usereditable="true">
      <Name>Text</Name>
      <Value default="true">$(User) $(Time)</Value>
    </Argument>
    <Argument usereditable="true">
      <Name>Transparency</Name>
      <Value default="true">30</Value>
    </Argument>
    <Argument usereditable="true">
      <Name>FontName</Name>
      <Value default="true">Sitka Text</Value>
    </Argument>
    <Argument usereditable="true">
      <Name>FontSize</Name>
      <Value default="true">36</Value>
    </Argument>
    <Argument usereditable="false">
      <Name>TextColor</Name>
      <Value default="true">Black</Value>
      <Value default="false">Red</Value>
      <Value default="false">Lime</Value>
      <Value default="false">Blue</Value>
      <Value default="false">Yellow</Value>
      <Value default="false">Cyan / Aqua</Value>
      <Value default="false">Magenta / Fuchsia</Value>
      <Value default="false">Gray</Value>
      <Value default="false">Dim Gray</Value>
      <Value default="false">Maroon</Value>
      <Value default="false">Olive</Value>
      <Value default="false">Green</Value>
      <Value default="false">Purple</Value>
      <Value default="false">Teal</Value>
      <Value default="false">Navy</Value>
    </Argument>
    <Argument usereditable="false">
      <Name>Rotation</Name>
      <Value default="true">Anticlockwise</Value>
      <Value default="false">Clockwise</Value>
    </Argument>
  </Arguments>
</Obligation>

<!-- Continued on the next page -->

```

XML code for configuration.xml (Continued..)

```
<!-- Continued from the previous page -->

    <Argument usereditable="false">
      <Name>Density</Name>
      <Value default="true">Normal</Value>
      <Value default="false">Dense</Value>
    </Argument>
  </Arguments>
</Obligation>
.....
```

For more details refer to [Configuring Rights Management Obligation](#).

After you have configured the obligation for your Control Center deployment, you can use the custom obligation while creating policies in Policy Studio.

☒ Custom Obligation

NameOB\_OVERLAY

Text\$(User) \$(Time)

Transparency30

FontNameSitka Text

FontSize36

TextColorBlack

RotationAnticlockwise

DensityNormal

The following table lists the attributes which are included in the OB\_OVERLAY custom obligation:

Attribute	Description
Text	This is the text you want to display as the watermark. You can also include \n to include a line break. \$(User) \$(Time) displays the current user's logon name and current Rights Management Server time at which the file is being viewed.
Transparency	Type the transparency level of the watermark. The default value is set to 30. This setting allows you to change how opaque or transparent the overlay is. Increasing the number makes the overlay more transparent. You can type any number between 0-100, where 0 represents fully opaque and 100 is fully transparent.

Attribute	Description
FontName	Type the font name in which you want to display the watermark. The default font name is Sitka Text.
FontSize	Type the font size in which you want to display the watermark. The default size is 36.
TextColor	Select the color in which you want to display the watermark. The default value is <b>Black</b> .
Rotation	Select the direction of rotation for your watermark. The default value is <b>Anticlockwise</b> .
Density	Select how dense you want the displayed watermark to be. The default value is <b>Normal</b> . If you want to increase the density of the watermark displayed on your NXL protected documents, you can set this value to <b>Dense</b> . <b>NOTE:</b> This field of the custom obligation is only handled by Rights Management Server. If your policy is enforced by Rights Management Client, then this field is ignored.

### Config File based Watermark

If you want to include a static watermark in all of your documents, then follow the steps indicated below:

In Rights Management Server, navigate to the `<RMS_DATA_DIR>`, and in the `RMSConfig.properties` file you can specify the following parameters:

Parameter	Description
IMAGE_WATERMARK	The value of this parameter is displayed as the watermark on the user's NXL protected document. You can also specify the following value to display the user's name: \$(User) You can specify the following value to display time: \$(Time)
WATERMARK_FONT_NAME	Set the value of this parameter to specify the font in which you want your watermark to be displayed. The default value is Sitka Text.

Parameter	Description
WATERMARK_DATE_FORMAT	<p>If you have specified this attribute value in any of your policies (via Policy Studio) then it will be ignored. Rights Management Server uses only the value specified for this attribute in the <code>RMSConfig.properties</code> file.</p> <p>Set the value of this parameter to specify the format of the date you want to display as part of your watermark. You can specify this as:</p> <p><code>yyyy-MM-dd</code></p> <p>This date format can also be any supported date and time pattern supported by java, as listed at this <a href="#">web link</a>.</p> <p>The default value is:</p> <p><code>EEE MMM dd HH:mm:ss yyyy</code></p> <p>The above default value displays the following sample value:</p> <p><code>Wed Oct 16 00:00:00 2013</code></p> <p><b>NOTE:</b> If you specify the incorrect date format then this will display the default value format indicated above.</p>
WATERMARK_FONT_SIZE	<p>Set the value of this parameter to specify the font size of your watermark. The font size is in pixels.</p> <p>The default value is 36.</p>
WATERMARK_FONT_COLOR	<p>Set the font color for your watermark. You can specify font colors as Black, Red, Lime, Blue, Yellow, Cyan, Magenta, Gray, Dim Gray, Maroon, Olive, Green, Teal, Purple, and Navy.</p> <p>The default value is Black.</p>
WATERMARK_FONT_TRANSPARENCY	<p>Set the transparency level percentage of your watermark. You can specify a value between 0 (fully opaque) and 100 (invisible).</p> <p>The default value is 30.</p>
WATERMARK_ROTATION	<p>Set the rotation direction of your watermark. You can specify the value as either Clockwise or Anticlockwise.</p> <p>The default value is Anticlockwise.</p>
WATERMARK_DENSITY	<p>Set the density of your watermark. you can specify the value as either Normal or Dense.</p>

**Note:** It is recommended that you specify your watermarks using custom obligations in your policies (in Policy Studio). This ensures that your watermarks are displayed consistently across all NextLabs endpoint software and not just Rights Management Server.

**Note:** If the font specified for the watermark in your policy or the `RMSConfig.properties` file is not installed on the Rights Management Server, Arial font is used instead.

### Policy versus Config File based Watermark

If you specify your watermarks in both policies and the `RMSConfig.properties` file, then the watermark information specified in your policy's custom obligation takes precedence.

If a user accessing a NXL protected document does not trigger any policy (which obligates the watermark to be displayed), then the watermark is displayed based on the `RMSConfig.properties` file.

### **Configuring the Session Timeout Duration**

Rights Management Server allows you to specify a minimum number of minutes before your Rights Management Server web portal session is terminated. This allows you to prevent inadvertent use of Rights Management Server by unauthorized personnel if the actual user has forgotten to log off or is not present.

1. Login to the Rights Management Server web portal.
2. Click **Configuration**.
3. In the **GENERAL** section, enter the number of minutes in the **Session Timeout** field.
4. Click **SAVE**.

## Configuring Rights for Control Center

NextLabs Rights Management Server supports the following Rights for policies deployed via NextLabs Control Center:

- Open (specified as `RIGHT_VIEW`)
- Print (specified as `RIGHT_PRINT`)
- PMI (specified as `RIGHT_VIEW_CAD_PMI`)

*Note:* Product and Manufacturing Information (PMI) rights are only supported for CAD files (excluding VDS files).

In order to ensure that the above Rights are available for use (in your Action Components) in policies created in Policy Studio, you must insert the following xml code into the `<ActionList>` node of the `configuration.xml` file (in NextLabs Control Center):

```
<ActionList>
...
  <Action>
    <Name>RIGHT_VIEW</Name>
    <DisplayName>Right View</DisplayName>
    <ShortName>R0</ShortName>
    <Category>Access</Category>
  </Action>

  <Action>
    <Name>RIGHT_PRINT</Name>
    <DisplayName>Right Print</DisplayName>
    <ShortName>R2</ShortName>
    <Category>Access</Category>
  </Action>

  <Action>
    <Name>RIGHT_VIEW_CAD_PMI</Name>
    <DisplayName>Right PMI</DisplayName>
    <ShortName>PM</ShortName>
    <Category>Transform</Category>
  </Action>
...
</ActionList>
```

After you have inserted these actions into the configuration file, logout of Policy Studio and restart NextLabs Control Center.

For more information about creating Action components in Policy Studio, which can be used in your policies, refer to the *Defining Action Components* section of the NextLabs Policy Studio User Guide.



## Configuring Rights Management Obligation

**Obligations** are events that occur as a result of a policy being enforced. To enable any pre-defined obligation, you must first register it with the system, which means editing the NextLabs Control Center's `configuration.xml` file.

Follow these steps to configure Rights Management obligations:

1. Use Notepad to open the `product.xml` file supplied by NextLabs support. This file include all obligations, special actions, and resource attributes required for the NextLabs product.
2. Locate the obligations section in the `product.xml` file and copy them to the clipboard.
3. Use Notepad to open the main configuration file, `configuration.xml`, on the Control Center host. By default it is located at:

```
[Install Directory]\NextLabs\Policy  
Server\server\configuration
```

4. Locate the `<Obligations></Obligations>` section, and paste the obligations into the main configuration file.
5. Save the changes to the `configuration.xml` file and restart the Policy Server.

*Note:* If you have deployed multiple ICENET servers, you must restart the ICENET windows service as well.

After you complete this configuration and restart the Policy Server, the obligations are mapped to the actual executable path and name, and the Display Names you entered display in Policy Studio in a drop-down list in the Obligations area. When you apply the obligations to the policy, are able to supply parameters that specify what the obligation does.

---

## Configuring the Rights Management Client

The NextLabs Rights Management Client enables you to view pdf and office documents in their respective native applications in a secure manner.

In the Rights Management Client, with the appropriate rights the user can not only view a NXL protected document but also do more. This includes but is not limited to making copies, printing, editing and taking screen shots of the document.

In NextLabs Rights Management Server you and Users can download the NextLabs Rights Management Client (RMC) installation package via the RMS Administrator console.

However, to make the Rights Management Client installation package available for download you must specify the file path of the RMC installation package in the `RMSConfig.properties` file.

### Specifying the RMC package location

1. In the `<RMS_DATA_DIR>`, open the `RMSConfig.properties` file in a word editor.
2. Locate the `RMC_PACKAGE_ZIP_PATH` and set the explicit file path for the Rights Management Client installation package. For example:

```
RMC_PACKAGE_ZIP_PATH=C:/TEMP/RMC_PACKAGE.ZIP
```

3. Save your changes and restart Rights Management Server.

### Downloading the Rights Management Client

1. Log in to the Rights Management Server Administrator console.
2. Go to any page, scroll down, and select **Download Rights Management Client**.

### Configuring RMC\_Classification.xml

1. In the `<RMS_DATA_DIR>`, open the `RMC_CLASSIFICATION.XML` file in a text editor. The file contains sample values.
2. Update the sections in the `RMC_Classification.xml` file with your own data. For more information about configuring the `RMC_CLASSIFICATION.XML` file, refer to the Rights Management Client Administrator's Guide.

### Configuring Local or External Login Credentials for RMC

You can configure the RMS configuration file to allow the users to log in to RMC using the local Windows login credentials or using the external login credentials. Perform the following steps as shown below.

1. In the `<RMS_DATA_DIR>`, open the `RMSConfig.properties` file in a text editor.

2. If you want to configure RMC for an external login authentication, enter the **RMC\_AUTH\_MODE** as **external** otherwise for the local Windows authentication, enter the **RMC\_AUTH\_MODE** as **local** or keep this field empty. By default, RMC uses the local authentication mechanism.

---

## Configuring RMS Memory Settings

1. Stop the Rights Management Server.
2. Configure the initial and maximum memory pool sizes as shown below:
  - For Windows:
    - Go to the `<RMS_INSTALL_DIR>\external\tomcat\bin` directory.
    - Open `rms.exe`.
    - Go to the **Java** tab.
    - Update the **Initial memory pool** and the **Maximum memory pool** fields. It is recommended to set a value of at least 1024 MB for the Maximum memory pool.
  - For Linux:
    - Go to the `/opt/nextlabs/RMS/external/tomcat/bin` directory.
    - Open the `setenv.sh` file using an editor.
    - Remove the comment from `export JAVA_OPTS="-Xms128M -Xmx-256M"` and modify the values.
3. Start the Rights Management Server.

## Importing Your Own SSL Certificates for Rights Management Server

By default, RMS uses a self-signed certificate for SSL connections. If you wish to use your own certificate from a Certified Authority, perform the following steps.

1. Stop the Rights Management Server.
2. On the Windows or Linux server, open the `server.xml` file from the `<RMS_INSTALL_DIR>\external\tomcat\conf` directory.
3. Locate the SSL Connector component.
4. Update the fields `keystoreFile`, `keystorePass` and `keystoreType` as shown the example below.

```
<Connector port="8443" protocol="org.apache.coyote.http11.Http11NioProtocol" SSLEnabled="true"
    keystoreFile="C:\ProgramData\NextLabs\RMS\datafiles\cert\rms_tomcat_keystore.jks"
    keystorePass="changeit"
    keystoreType="JKS"
    maxThreads="150" scheme="https" secure="true"
    clientAuth="false" sslProtocol="TLS"
    maxPostSize="524288000"
    URIEncoding="UTF-8"
/>
```

5. Start the Rights Management Server.



### Adding a Repository

Rights Management Server allows you to add repositories which contain information you want to collaborate on with stakeholders that don't have any NextLabs Endpoint software installed.

NextLabs protected documents that can only be viewed with NextLabs Endpoint software can be shared with personnel in a secure manner without the need for propriety software installed on their machines.

Rights Management Server currently supports SharePoint, SharePoint Online, Google Drive, and Dropbox repositories

You must first add your respective repository to the Rights Management Server before you can begin authorizing external personnel to view your NXL protected documents.

1. Log in to the Rights Management Server Administrator console.
2. Click **Manage Repositories**.
3. Click **Add Repository**.
4. Select one of the following from the **Repository** list:

Repository Name	Description
SharePoint	If your files reside on a Microsoft SharePoint portal, select this option. <b>NOTE:</b> In your Microsoft SharePoint deployment you must configure an NXL file filter. This filter allows SharePoint to index all NXL files. For more information, refer to <a href="#">Configuring a NXL Filter for MS SharePoint</a> .
Dropbox	If your files reside in Dropbox, select this option. <b>NOTE:</b> You must setup your Rights Management Server for adding a Dropbox repository prior to adding the repository. This only needs to be done once per deployment. For more information refer to <a href="#">Configuring Rights Management Server for Dropbox Repositories</a> .
Google Drive	If your files reside in Google Drive, select this option. <b>NOTE:</b> You must setup your Rights Management Server for adding a Google Drive repository prior to adding the repository. This only needs to be done once per deployment. For more information refer to <a href="#">Configuring Rights Management Server for Google Drive</a> .

Repository Name	Description
OneDrive	If your files reside in OneDrive, select this option. <b>NOTE:</b> You must setup your Rights Management Server for adding a OneDrive repository prior to adding the repository. This only needs to be done once per deployment. For more information refer to <a href="#">Configuring Rights Management Server for Microsoft OneDrive</a> .

- If you selected **Microsoft SharePoint**, then type the **SharePoint URL** and **Repository Display Name**.

*Note:* It is recommended that you add a SharePoint URL which points to a Site. Currently Rights Management Server does not support SharePoint URLs which point to a library, list or folder.

*Note:* If you specify the **SharePoint URL** as an IP address, then you must ensure that your SharePoint Administrator has the appropriate alternate access mapping setup for this IP address. For more information, refer to [Configuring Alternate Access Mapping](#). If you are specifying a SharePoint URL using "https", then you must specify the port number as well (for example, https://mysharepoint.com:443). If you are using a self-signed certificate then refer to [Exporting a Self-Signed Certificate to Rights Management Server](#).

- If you selected **Dropbox**, **Google Drive**, or **OneDrive**, then type the **Repository Name**.
- Click **SAVE**.



---

## Integrating with SharePoint

Rights Management Server can be used to view NXL protected documents hosted on SharePoint sites. This ensures that all NXL protected documents on your SharePoint site are viewed in a secure manner without the need to have any NextLabs proprietary software installed.

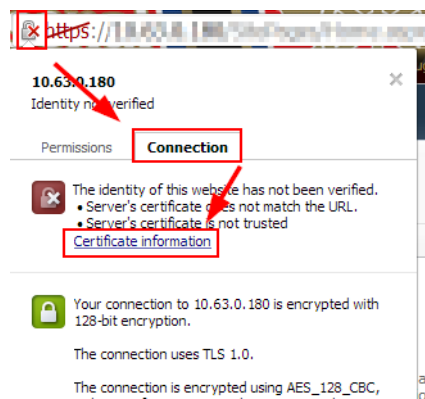
Rights Management Server can integrate with Microsoft SharePoint as a menu option available on your SharePoint sites. You can integrate Rights Management Server with both Microsoft SharePoint Online (for more information, refer to [Integrating with SharePoint Online](#)) or Microsoft SharePoint On-Premise (for more information, refer to [Integrating with SharePoint On-Premise](#)).

## Exporting a Self-Signed Certificate to Rights Management Server

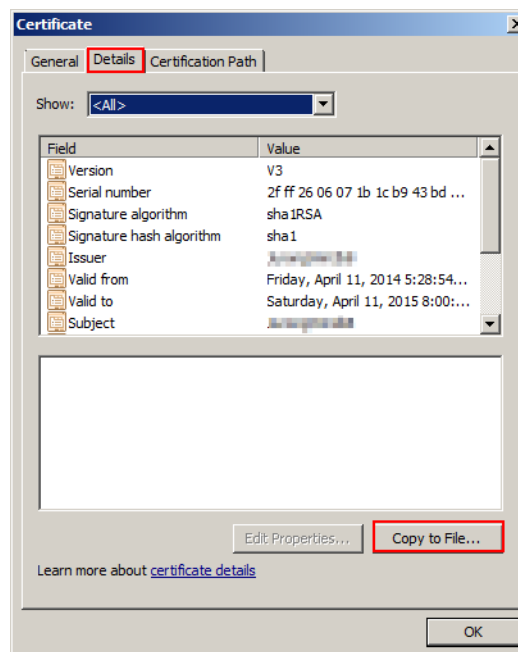
If you are attempting to add a repository URL which contains https or a secure SharePoint repository (which uses self signed security certificates) then you must export the security certificate and add it to the Rights Management Server TrustStore.

*Note:* If you are using security certificates issued by a third party authority then you can skip this section since this will not apply to your scenario.

1. In your web browser click the secure certificate icon, and click the **Certificate Information** hyper link.



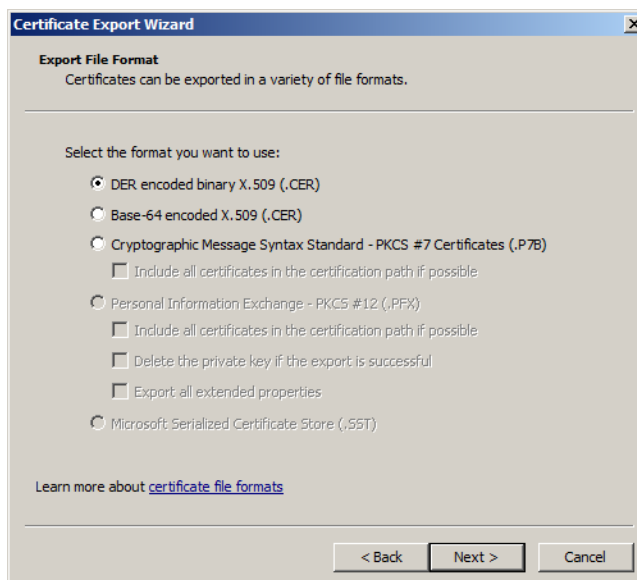
2. In the Certificate window, select the **Detail** tab and click **Copy to File**.



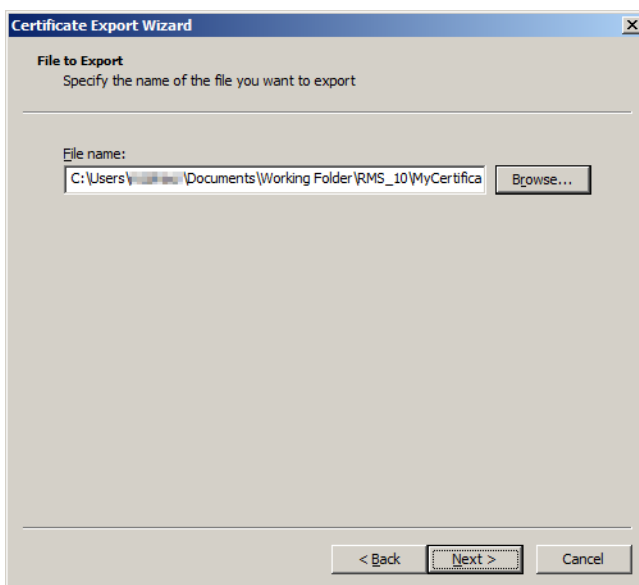
3. In the Certificate Export Wizard, click **Next**.



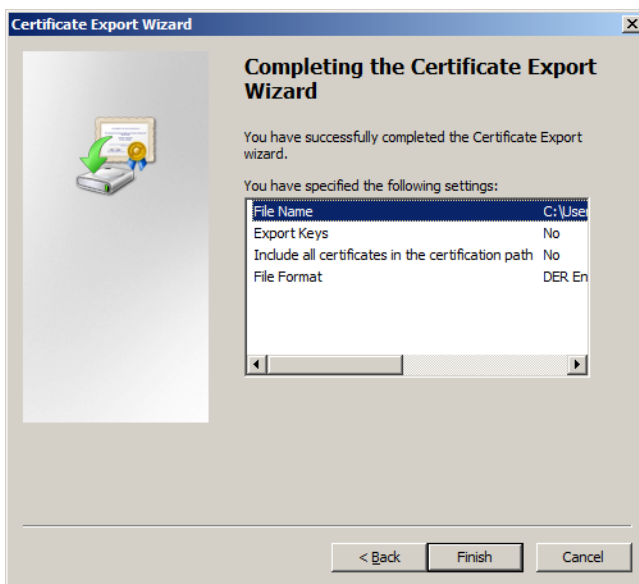
4. Select **DER encoded binary X.509 (.CER)** and click **Next**.



5. Click **Browse** and select the directory path where you want to save your certificate, and click **Next**.



6. Click **Finish**.



7. Copy your Certificate to Rights Management Server.
8. In your Rights Management Server machine, navigate to the Windows command prompt icon, right-click and select **Run as Administrator**.
9. Add your certificate to the KeyStore for the JRE being used by Apache Tomcat using the following command:

```
keytool -importcert -file <windows_file_path_for_your_certificate> -keystore <windows file path for your JRE keystore> -alias <your_keystore_alias>
```

**An example of such a command for jdk 1.7.0\_45 installed at C:\Program Files would be:**

```
keytool -importcert -file C:\temp\joe\rms-sp13cert.cer -keystore C:"\Program Files\Java\jdk1.7.0_45\jre\lib\security\cacerts" -alias rms-sp13joe
```

10. Review your certificate details and type Yes, then press <Enter> add this certificate to your TrustStore.



---

### Introduction

Microsoft SharePoint Online is a web based enterprise software that allows organizations to share information internally and externally.

You can deploy the Rights Management Server-SharePoint Online App which handles all file access requests for any NXL protected file on your SharePoint Online deployment.

SharePoint redirects the file access request to Rights Management Server which then authenticates the User prior to decrypting it and displaying it in the User's web browser window.

Currently Rights Management Server is only supported to work with Microsoft SharePoint Online and SharePoint 2013. You can create your SharePoint Online App in Rights Management Server, but you need to register your SharePoint Online App first.

This chapter describes configuration steps for integrating Rights Management Server with SharePoint Online. Note that your configuration will be specific to your product implementation.

Configuration procedures are broken into the following sections:

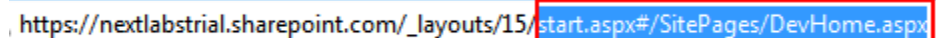
- [Registering your SharePoint Online App](#)
- [Creating your SharePoint Online App](#)
- [Deploying your SharePoint Online App](#)

## Registering your SharePoint Online App

Before you can use Rights Management Server to create your SharePoint Online App you must register your SharePoint Online App. The registration process generates Client and Secret Client IDs while also saving the public listed IP address of the machine on which your Rights Management Server deployment is hosted.

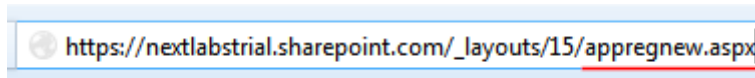
*Note:* The following steps are applicable if you want to register a High-Trust App for SharePoint Online as well.

1. Navigate to your SharePoint Online site in your web browser.
2. Select the URL of your site in the address bar and remove part of the address after `layouts/15/` as indicated below:



`https://nextlabstrial.sharepoint.com/_layouts/15/start.aspx#/SitePages/DevHome.aspx`

3. Append the URL in your address bar with `appregnew.aspx` as indicated below and press <Enter>:



`https://nextlabstrial.sharepoint.com/_layouts/15/appregnew.aspx`

4. Select **An app running on a web server** for your **App Type** to indicate the type of app you want to create.

App Type:

- ☒ An app running on a web server  
☐ An app running on a client machine

5. Click **Generate** to create a **Client Id** and note it down.

Client Id:

Generate

*Note:* Copy and Save this **Client Id** value. This value is used for creating your SharePoint Online app in the Rights Management Server user interface.

6. Click **Generate** to create a **Client Secret** value.

Client Secret:

Generate



**Note:** The Client Secret value is used for your SharePoint Online App. This value expires after one year. Before you attempt to regenerate it, you must remove the **Client Id** and SharePoint Online App certificate name from your SharePoint deployment. Then you can update the **Client Id** value for your app. For more information, refer to [Removing an Expired Client Id and Certificate Name](#) and [this MSDN article](#).

7. Type the following details:

Field	Description
Title	your app name
App Domain	Publicly listed IP address or web address for your Rights Management Server, for example 10.168.23.28 or www.MyMachine.com <b>NOTE:</b> If the port number being used is not 443 then you must specify the port number too with this value, for example www.MyMachine.com:5555 or 10.168.23.28:8443
Redirect URI	Publicly listed IP address or web address for your Rights Management Server with the appropriate protocol included, for example https://10.168.23.28:8443 or https://MyMachine.com:8443 <b>NOTE:</b> If the port number being used is not 443 then you must specify the port number with this value, for example www.MyMachine.com:5555 or 10.168.23.28:8443

8. Click **Create**.

9. Copy and save the information displayed on your screen and click **OK**.

The app identifier has been successfully created.

Client Id: 2d58a2ee-cac8-4ad7-a71b-834efc0b54f2

Client Secret: JvegD+u9MV8KhE/NABlUqlaVMw2/dkS5jsYTh7nwo=

Title: MySecureCollaborationApp

App Domain: www.MyMachine.com

Redirect URI: https://MyMachine.com

## Creating your SharePoint Online App

1. Change the extension of your SharePoint Online App file from .app to .zip. For example if your SharePoint Online App file is `Secure_Collaboration_SP_Online_App.app` then rename it to `Secure_Collaboration_SP_Online_App.zip`.

2. Copy your SharePoint Online App file to the `<RMS_DATA_DIR>`.


**Note:** If you want to copy the App file to some other location then you must specify this in the `RMSConfig.properties` file (located in the `<RMS_DATA_DIR>`). The SharePoint Online App file path must be specified under the variable name, `SP_APP_PATH_ONLINE`. A sample value in the `RMSConfig.properties` file could be:

```
SP_APP_PATH_ONLINE=C:/Users/joe/Desktop/SecureCollaboration_SP_Online_App.zip
```

3. Login to the Rights Management Server Administrator console.
4. Click **Service Providers**.
5. In the **Cross-Launch Apps** section, move the cursor over **SharePoint Online Cross-Launch** and click **Configure**.
6. Enter the following details:

Field	Description
App Name	Enter a unique name to identify the SharePoint app.
App Key	This is the key value that was generated during the SharePoint Online app registration. For more details, see <a href="#">Registering your SharePoint Online App</a> .
App Secret	This is the Client Secret of the SharePoint App that you want to configure.  <b>NOTE:</b> The App Client Secret value expires after one year. You must regenerate it after one year and update it for your app. Before you attempt to regenerate it, you must remove the <b>Client Id</b> and SharePoint Online App certificate name from your SharePoint deployment. Then you can update the <b>Client Id</b> value for your app. For more information, refer to <a href="#">Removing an Expired Client Id and Certificate Name</a> and <a href="#">this MSDN article</a> .
Redirect URL	Enter the URL of the server hosting Rights Management Server application.
App Menu Display Text	Enter a unique menu name for user to view the rights protected file via RMS.

7. Click **SAVE**.
8. Go to **Service Providers > Configured Providers**.
9. Move the cursor over **SharePoint Online Cross-Launch**.

10. Click the download icon for your SharePoint Online App .

*Note:* The SharePoint Online App is downloaded as a zip file.

11. Change the extension of your zip file to .app.

### **Deploying your SharePoint Online App**

Upload your SharePoint Online App to your SharePoint Online App Catalogue (for more information refer to [Add apps to the App Catalog](#)). You can then install this app for each of the SharePoint Online sites you want to use it for. For more information, refer to [Add apps for SharePoint to a SharePoint 2013 site](#).

This SharePoint Online App allows you to view your SharePoint Online NXL protected files in the Rights Management Server Server.

*Note:* If you have just deleted an older version of the SharePoint Online App, then you must wait at least 5 minutes for the action to take effect before attempting to deploy the latest version of your app.

## Removing an Expired Client Id and Certificate Name

Each time you register a SharePoint Online App, the generated **Client Id** value is valid only for a year after which it must be updated.

Before you attempt to generate a new **Client Id** value for your SharePoint Online App, you must remove the expired **Client Id** as well as the certificate name of your SharePoint Online App.

Type the following Microsoft Windows Powershell commands (on your Microsoft SharePoint deployment) to remove the expired **Client Id** value and certificate name:

```
./HighTrustConfig-ForSingleApp.ps1 -certPath <File path for  
your certificate file> -certName <your certificate name> -  
SPAppClientID <the expired Client Id> -  
TokenIssuerFriendlyName <the alias for your app>
```

```
Remove-SPTrustedRootAuthority -Identity <your certificate  
name>
```

```
Remove-SPTrustedSecurityTokenIssuer -Identity <the alias for  
your app>
```

The following is a sample Microsoft Powershell command:

```
./HighTrustConfig-ForSingleApp.ps1 -certPath  
"C:\Certs\spstg.cer" -certName "spstglamvcccomDomainCert" -  
SPAppClientID "4b553b48-6b29-454c-bd4c-6d5ac898f484" -  
TokenIssuerFriendlyName "myapp"
```

```
Remove-SPTrustedRootAuthority -Identity  
"spstglamvcccomDomainCert"
```

```
Remove-SPTrustedSecurityTokenIssuer -Identity "myapp"
```

---

### Introduction

SharePoint On-Premise refers to the stand alone deployment of SharePoint in your network. You can deploy Rights Management Server-SharePoint On-Premise Apps to integrate the ability to view NXL protected files via Rights Management Server. There are two apps that are deployed for Rights Management Server and SharePoint On-Premise integration:

- **SharePoint On-Premise app:**  
This app is created via the Rights Management Server UI. The app is uploaded to the SharePoint App Catalogue and handles any file access requests for Rights Management Server. It forwards these requests to the SharePoint On-Premise web app.
- **SharePoint On-Premise Web App:**  
The SharePoint On-Premise web app can be obtained from the same location as your Rights Management Server package. This web app acts as a information broker between Rights Management Server and the SharePoint On-Premise App.

The following sections refer to the steps involved when integrating with your SharePoint On-Premise deployment.

*Note:* Rights Management Server currently supports only SharePoint 2013 for SharePoint On-Premise.

This chapter describes configuration steps for integrating Rights Management Server with SharePoint On-Premise. Note that your configuration will be specific to your product implementation.

This configuration procedure is broken into the following sections:

- [Prerequisites](#)
- [Registering the High-Trust App](#)
- [Configure the Remote Web Server with the Certificate](#)
- [Configuring SharePoint to Use the Certificate](#)
- [Modifying the SetParameters File](#)
- [Modifying your Web Server's web.config File](#)
- [Publishing Remote Web App in SharePoint](#)
- [Configuring Protocol Binding for the Web App](#)

- [Configuring Authentication for the Web App](#)
- [Creating your SharePoint On-Premise Apps](#)

## Deploying the Provider Hosted App

To deploy the Rights Management Server hosted app to your SharePoint deployment refer to the latest steps on the Microsoft website under the article [How to: Package and publish high-trust apps for SharePoint 2013](#).

The following sections have been documented based on information from the above mentioned URL. It is recommended that you first refer to the official Microsoft website to note down any discrepancy against the steps listed below.

*Note:* After you have completed the steps indicated below you must upload and install your high-trust app. For more information, refer to [Deploying your SharePoint Online App](#).

### Prerequisites

- Ensure that the Microsoft SharePoint Foundation Subscription Service has been started
- Ensure that the User Profile Service Application has been started
- Ensure that the App Management Service has been started
- Ensure that at least one User Profile has been created
- The App Catalogue has been created (using the Central Administrator page)
- IIS web server to host the remote web application (this can be the same server as SharePoint)
- A X.509 digital certificate for the remote web app of your high-trust app
- **Web Deploy** installed on the remote web application server

### Registering the High-Trust App

The app registration process for the High-Trust App is similar to that mentioned in [Registering your SharePoint Online App](#). You must perform these steps for your High-Trust App to register it before you move to the next section.

*Note:* You need the Site Collection Administrator to register your SharePoint Online App (i.e. generate the client id and client secret).

### Configure the Remote Web Server with the Certificate

You need to create two certificates (.pfx and .cer formats) and import them into IIS. This allows IIS to facilitate a high trust communication between SharePoint and the SharePoint On-Premise web app.

*Note:* If your Microsoft SharePoint deployment is using the https protocol, then you do not need to create new certificates (.pfx and .cer formats) and import them each time you deploy a new version of your Rights Management Server SharePoint App. You can continue to use the same certificates.

### Importing the .pfx Certificate

1. Create a folder to which the **ApplicationPoolIdentity** user of the remote web app has Read rights.

*Note:* By default, IIS assigns a user called **ApplicationPoolIdentity** to its web apps when they are created. This user cannot be given access to non-local files. If the certificate is not stored on the same server that is hosting the remote web app, then you need to change the app pool identity to a user that has Read rights to the non-local folder.

2. In IIS Manager, select the **ServerName** node in the tree view.
3. Double-click **Server Certificates**.
4. Select **Import** in the **Actions** pane on the right.
5. In the **Import Certificate** dialog box, click **Browse**.
6. Navigate to the .pfx file and then type the password of the certificate.
7. Check the option to allow this certificate to be exported and click **OK**.
8. In the **Server Certificates** list, right-click the certificate, and then select **Export**.
9. Export the file to the folder that you created (at the start) and type its password.

### Importing the .cer Certificate

1. In IIS manager, select the **ServerName** node in the tree view.
2. Double-click **Server Certificates**.
3. In **Server Certificates** view, double-click the certificate to display the certificate details.
4. In the **Details** tab, click **Copy to File launch Certificate Export Wizard**, and then click **Next**.
5. Select the default value **No** (do not export the private key) and then click **Next**.
6. Click **Next**.
7. Click **Browse** and select a folder.

*Note:* The .cer certificate is moved from this computer. Save the .cer file with the same name as the .pfx file.

8. Click **Next**.
9. Click **Finish**.



10. Restart Tomcat.

## Configuring SharePoint to Use the Certificate

Configuring SharePoint to use your certificates involves the following two processes.

### Distributing the .cer file to SharePoint

These steps need to be performed on every SharePoint server in your farm. You must use the same values for each server, for example, the same folder name.

1. Create a folder and be sure that the App Pool Identity for the following IIS app pools has Read rights to it:
  - SecurityTokenServiceApplicationPool
  - The app pool that serves the IIS web site that hosts the parent SharePoint web app for your test SharePoint website. For the SharePoint - 80 IIS website, the pool is called OserverPortalAppPool
2. Move the .cer file from the remote web server to this folder on your SharePoint server.

### Configuring the Certificate

The following steps configure the certificate as a trusted token issuer in SharePoint. It is performed just once (for each high-trust app for SharePoint) and can be done on any SharePoint server.

1. Create your high-trust configuration Windows PowerShell script.

*Note:* These scripts have been included in `SecureCollaboration_SPOnPremiseApp.zip` file (in the `scripts` folder: `HighTrustConfig-FOrSingleApp.ps1` and `SiteSubscriptions.ps1`). This zip file can be obtained from NextLabs Support.

2. Copy the script files to a SharePoint server.
3. Open the SharePoint Management Shell as an administrator and run the appropriate scripts.

*Note:* For more information about how to run the scripts, refer to the `readme.txt` file (included in the shell `scripts` folder mentioned above).

The registration of your certificate as a token issuer is effective immediately. It may take as long as 24 hours before all the SharePoint servers recognize the new token issuer. Running an `iisreset` on all the SharePoint servers ensures that they all recognize the issuer.

**Note:** Running `iisreset` is recommended only if you are sure that SharePoint user traffic is low, since running this method impacts users.

## Modifying the SetParameters File

The `Nextlabs.SC.SPHighTrustApp.Web.SetParameters.xml` file of your remote web app needs to be modified to contain new values for the following keys in the `<appSettings>` node:

Field	Description
IIS Web Application Name	This is the name of the SharePoint web app you have created in IIS
ClientId	This is the Client Id value that was generated during the app registration. For more details, see <a href="#">Registering your SharePoint Online App</a> .
ClientSigningCertificatePath	This is the full path and filename of the *.pfx file
ClientSigningCertificatePassword	This is the password that you gave the certificate
IssuerId	This is the GUID of the token issuer (which must be lower case). Its value depends on the certificate strategy of the customer
AuthType	This is the type of authentication you are using. There are three supported types: WIN (Windows Authentication), ADFS (Active Directory Federation Services), and FBA (Forms Based Access). The default value is WIN.

**Note:** If the high trust app for SharePoint has its own certificate that it is not sharing with other apps for SharePoint, the `IssuerId` is the same as the `ClientId`.

The following is a sample

`Nextlabs.SC.SPHighTrustApp.Web.SetParameters.xml` file:

Nextlabs.SC.SPHighTrustApp.Web.SetParameters.xml
<pre>&lt;?xml version="1.0" encoding="utf-8"?&gt; &lt;parameters&gt;   &lt;setParameter name="IIS Web Application Name" value="SCHighTrustApp" /&gt;   &lt;setParameter name="ClientId" value="c1c12d4c-4900-43c2-8b89-c05725e0ba30" /&gt;   &lt;setParameter name="ClientSigningCertificatePath" value="C:\MyCerts\MyCert.pfx" /&gt;   &lt;setParameter name="ClientSigningCertificatePassword" value="mypassword6392" /&gt;   &lt;setParameter name="IssuerId" value="c1c12d4c-4900-43c2-8b89-c05725e0ba30" /&gt;   &lt;setParameter name="AuthType" value="WIN" /&gt; &lt;/parameters&gt;</pre>

**Note:** There is no `ClientSecret` key included for your High-Trust app in SharePoint, as indicated above.

## Modifying your Web Server's web.config File

In order to support ADFS (Active Directory Federation Services) and FBA (Forms Based Authentication), you must add the xml code listed below to your IIS web server's `web.config` file (located in the `AppWeb.deploy` folder of `SecureCollaboration_SPOnPremiseApp.zip` file). You must add the following xml code in the `<appSettings>` section:

web.config.xml
<pre>&lt;add key="AuthType" value="ADFS" /&gt; &lt;add key="IdentityClaimType" value="SMTP"/&gt; &lt;add key="ClaimProviderType" value="SAML"/&gt; &lt;add key="TrustedProviderName" value="your SAML Provider"/&gt; &lt;add key="MembershipProviderName" value="your FbaMember"/&gt;</pre>

**Note:** Regardless of which authentication type you specify in the above xml code, you must ensure all of the above parameters are listed. For a particular authentication type that you are not using you can specify any place holder value.

Which contains the following values:

Field	Description
<b>AuthType</b>	This is the type of authentication you are using. There are three supported types: WIN (Windows Authentication), ADFS (Active Directory Federation Services), and FBA (Forms Based Access). The default value is WIN.
<b>IdentityClaimType</b>	This is the claim type to identify the user to SharePoint: SMTP (Simple Mail Transfer Protocol), UPN (User Principal Name), and SIP (Session Initiation Protocol). The default value is SMTP.
<b>ClaimProviderType</b>	This is the claim provider type: FBA (Forms Based Access), SAML (Security Assertion Markup Language). The default value is SAML.
<b>TrustedProviderName</b>	This is the Trusted Provider Name (if your SharePoint site is using SAML authentication, then you must specify this). This is the name of your SPTrustedSecurityTokenIssuer.
<b>MembershipProviderName</b>	This is the Membership Provider Name (if your SharePoint site is using SAML authentication, then you must specify the name of the "ASP.NET Membership provider name". This is the value you set up in the authentication providers dialog for your web application).

## Publishing Remote Web App in SharePoint

1. Copy all the files in `AppWeb.deploy` to a folder on the remote server.

**Note:** This folder is included in the `SecureCollaboration_SPOnPremiseApp.zip` file. This zip file can be obtained from NextLabs Support.

2. In this folder, open the `NextLabs.SC.SPHighTrustApp.Web.deploy-readme.txt` file, and follow the instructions in the file to install the web app using the `Nextlabs.SC.SPHighTrustApp.Web.deploy.cmd` file.

## Configuring Protocol Binding for the Web App

*Note:* You may need to create a hosted app web site on the remote server's IIS first.

1. In IIS Manager, highlight the new website in the Connections pane.

*Note:* If the new web app is a child of the Default Web Site, select the Default Web Site and carry out the following steps for the Default Web Site.

2. Click **Bindings** in the Actions pane.
3. In the Add Site Binding dialog box, click **Add**.
4. Select **HTTPS** in the **Type** list.
5. Select **All Unassigned** in the **IP address** list.
6. Type the port number in the **Port** field.

*Note:* If you specified a port in the app domain when you registered the app for SharePoint, then you must use the same number here. If you did not specify any port number then type 443.

7. In the SSL certificate list, select the certificate that you used to configure the server in [Configuring the Certificate](#) above.
8. Click **OK**.
9. Click **Close**.

## Configuring Authentication for the Web App

When a new web app is installed in IIS, it is initially configured for anonymous access, but almost all high trust apps for SharePoint are designed to require authentication of users. Therefore this needs to be changed.

1. In IIS Manager, select the web app in the Connections pane. It will be either a peer website of the Default Web Site or a child of the Web Site.
2. Double-click the Authentication icon in the center pane to open the Authentication pane.
3. Select **Anonymous Authentication** and then click **Disable** in the Actions pane.
4. Select the authentication system that the web app is designed to use and click **Enable** in the Actions pane.

*Note:* The web app is using Windows Authentication, therefore this is the option you must enable.

If you are using the generated code files unmodified, you also need to configure the authentication provider with the following steps:

## Creating your SharePoint On-Premise Apps

1. Select **Windows Authentication** in the Authentication pane.
2. Click **Providers**.
3. In the Providers dialog, ensure that NTLM is listed above Negotiate.
4. Click **OK**.

1. Copy your SharePoint On-Premise App file to the [<RMS\\_DATA\\_DIR>](#).

*Note:* If you want to copy the App file to some other location then you must specify this in the `RMSConfig.properties` file (located in the [<RMS\\_DATA\\_DIR>](#)). The SharePoint On-Premise App file path must be specified under the variable name, `SP_APP_PATH_ON_PREMISE`. A sample value in the `RMSConfig.properties` file could be:


```
SP_APP_PATH_ON_PREMISE=C:/Users/joe/Desktop/SecureCollaboration_SP_OnPremise_App.zip
```

2. Login to the Rights Management Server Administrator console.
3. Click **Service Providers**.
4. In the **Cross-Launch Apps** section, move the cursor over **SharePoint Cross-Launch**.
5. Select **Configure**.
6. Enter the following details:

Field	Description
App Name	A unique name to identify the app.
App Client Id	This is the <b>Client Id</b> value that was generated during the SharePoint web app registration. For more details, see <a href="#">Registering your SharePoint Online App</a> .
App Client Secret	This is the Client Secret of the SharePoint App that you want to configure.
Remote Web Application URL	This is the URL of your SharePoint On-Premise web app that you have deployed on your IIS. You must append the following to it: <code>/Pages/Default.aspx</code> For example if your SharePoint Site App URL is: <code>https://myserver:4444</code> then you must type it as: <code>https://myserver:4444/Pages/Default.aspx</code> <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: <code>https://myserver/Pages/Default.aspx</code>
Redirect URL	The URL of the server hosting Rights Management Server application.
App Menu Display Text	The menu name shown to the user for viewing rights protected file.

7. Go to the **Service Providers > Configured Providers**.

8. Move the cursor over **SharePoint**.

9. Click the download icon for your SharePoint On-Premise App .

*Note:* The SharePoint On-Premise App is downloaded as a zip file.

10. Change the extension of your zip file to .app.

*Note:* SharePoint On-Premise App that must be uploaded to the App catalogue. For more information about deploying the SharePoint On-Premise App, refer to [Deploying your SharePoint Online App](#).

---

### Configuring Rights Management Server

This chapter describes configuration steps integrating Rights Management Server with Dropbox. Note that your configuration will be specific to your product implementation.

Configuration procedures are broken into the following sections:

- [Creating your Dropbox App for Rights Management Server](#)
- [Configuring your Dropbox App](#)

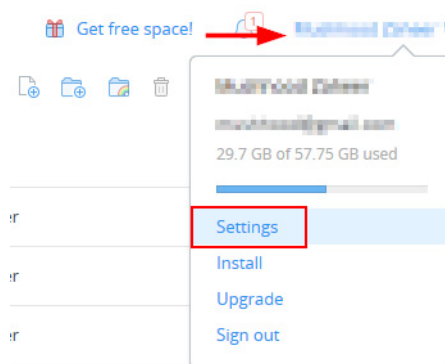
## Configuring Rights Management Server for Dropbox Repositories

### Creating your Dropbox App for Rights Management Server

Before you can begin adding Dropbox repositories to Rights Management Server you must create your Dropbox app which will interface with Rights Management Server to ensure that access to the repository is granted

*Note:* The steps indicated below need to be done only once per Rights Management Server deployment. You must perform these configuration steps to be able to successfully add Dropbox repositories to your Rights Management Server.

1. Login to the Dropbox website.
2. Click on your login name and then click **Settings**.



3. Scroll down to the bottom of the page and click the **Developers** link.

Dropbox	About us	Support	Community
Install	Dropbox Blog	Help Center	Referrals
Mobile	Our team	Get Started	Twitter
Pricing	Branding	Privacy & Terms	Facebook
Business	News	Copyright	<b>Developers</b>
Tour	Jobs	Contact us	



4. In the navigation links on the left hand side, click **App Console**.

Developer home

**App Console**

Drop-ins

Datastore API

Sync API

Core API

Developer guide

Branding guide

5. Review the Dropbox API terms and conditions, set the **I agree** check box and click **Submit**.

6. Select **Dropbox API app**.

Create a new Dropbox Platform app

What type of app do you want to create?

<input type="radio"/>  <b>Drop-ins app</b> Chooser or Saver	<input checked="" type="radio"/>  <b>Dropbox API app</b> Sync API, Datastore API, or Core API
--	--

7. Select **Files and datastores**.

What type of data does your app need to store on Dropbox?

<input checked="" type="radio"/> <b>Files and datastores</b>
<input type="radio"/> Datastores only

8. Select **No**.

Can your app be limited to its own, private folder?

<input type="radio"/> Yes — My app only needs access to files it creates.
<input checked="" type="radio"/> <b>No — My app needs access to files already on Dropbox.</b>

9. Select **All file types**.

What type of files does your app need access to?

<input type="radio"/> Specific file types — My app only needs access to certain file types, like text or photos.
<input checked="" type="radio"/> <b>All file types — My app needs access to a user's full Dropbox. Only supported via the Core API.</b>

## 10. Type your Dropbox app name.

Provide an app name, and you're on your way.

RMS app

11. Click **Create app**.

## Configuring your Dropbox App

1. After your Dropbox app has been created, click the **Settings** tab for the newly created app.



Developer home

App Console

Drop-ins

### RMS app

Settings

Details

2. In the **OAuth redirect URIs** field, type your Rights Management Server address in the following format:

<Your Rights Management Server name>:<Port number>/RMS/DBAuth/dbAuthFinish

For example:

https://Seletar:8443/RMS/DBAuth/dbAuthFinish

OAuth redirect URIs

https://seletar:8443/RMS/DBAuth/dbAuthFinis

Add

http:// allowed only for localhost URIs

**Note:** If your Rights Management Server user intends to access the Rights Management Server portal using a different URI than the one added here then after logging in to Rights Management Server the user would not be able to add their Dropbox repository for their Rights Management Server account. Therefore you must include the URI the user types to access the Rights Management Server portal in the above field. It is recommended you include all versions of the URI that your user types in order to access the Rights Management Server portal.

3. Click **Add**.


4. In the Settings tab, copy the **App Key** and **App Settings** values.

App key

yfsz5q17cpysikq

App secret

kmnizypckjpxi7

5. In the Rights Management Server web portal, click the **Settings**  > **Application Settings** menu.
6. Select **Personal Repo Settings** > **Dropbox Settings**.
7. Under **Dropbox Settings**, copy the **App Key** and **App Settings** values to the **Dropbox App Key** and **Dropbox App Secret** fields respectively.
8. Enter the redirect URL that was configured in the Dropbox Developer Console. The format of the URL is

`https://<RMS Address>:<port number>`

9. In the Dropbox website, under the **Settings** tab, click **Enable additional users**.

*Note:* This option allows up to 100 users to install the Dropbox app. If you skip this option then only 1 Dropbox user can install the app. If you want to support more than 100 users then you must apply for production status of your app with Dropbox.

Development users

Only you

Enable additional users



---

### Configuring Rights Management Server

This chapter describes configuration steps for integrating Rights Management Server with Google Drive.

The configuration procedures are broken into the following sections:

- [Creating your Google Drive App for Rights Management Server](#)
- [Configuring your Google Drive App](#)

## Configuring Rights Management Server for Google Drive

Using the Google Drive repository in RMS, users can view, and download the files they need but cannot push or edit the files.

Before you can begin adding Google Drive repositories to Rights Management Server you must create your Google Drive app which will interface with Rights Management Server to ensure that access to the repository is granted

*Note:* The steps indicated below need to be done only once per Rights Management Server deployment. You must perform these configuration steps in order to successfully add Google Drive repositories to your Rights Management Server.

## Creating your Google Drive App for Rights Management Server

1. Log in to <https://console.developers.google.com>.
2. Select the menu option, **Select a project > Create a project**.
3. Enter a project name, accept the terms, and click **Create**.

New Project

Project name ?

My Project

Your project ID will be poetic-archway-116709 ? Edit

Show advanced options...

Please email me updates regarding feature announcements, performance suggestions, feedback surveys and special offers.

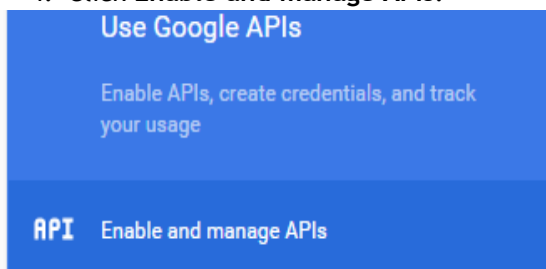
☐ Yes ☒ No

I agree that my use of any services and related APIs is subject to my compliance with the applicable Terms of Service.

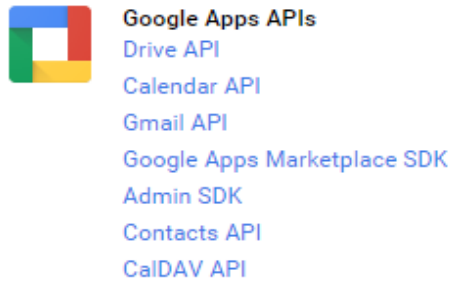
☐ Yes ☒ No

Create Cancel

4. Click **Enable and manage APIs**.



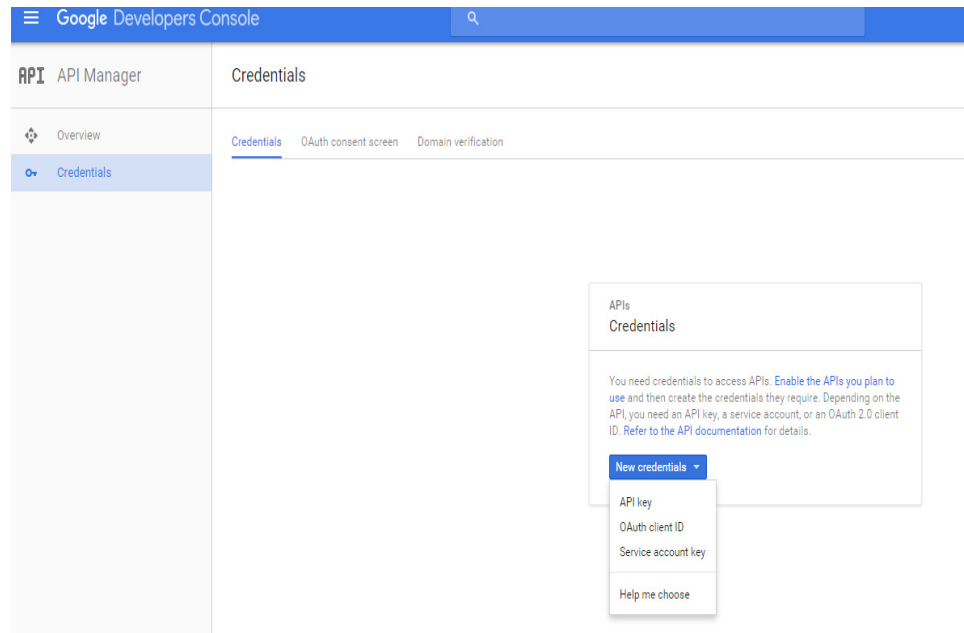
5. Select **Drive API**.



6. Click **Enable API**.

7. After enabling the API, select the **Credentials** menu on the left.

8. Select **New credentials > OAuth client ID**.



9. Select **Configure consent screen**.

## 10. Enter the product name and Save.

API Manager

Overview

Credentials

Credentials OAuth consent screen Domain verification

Email address

abeeshthomas@gmail.com

Product name shown to users

RMS

Homepage URL (Optional)

Product logo URL (Optional)

http://www.example.com/logo.png

This is how your logo will look to end users  
Max size: 120x120 px

Privacy policy URL (Optional)

Terms of service URL (Optional)

Save Cancel

## 11. Select Application type as Web application.

Create client ID - RMSDemo x

https://console.developers.google.com/apis/credentials/oauthclient?project=rmsdemo-1163

Google Developers Console

API Manager

Overview

Credentials

Create client ID

Application type

☒ Web application

☐ Android [Learn more](#)

☐ Chrome App [Learn more](#)

☐ iOS [Learn more](#)

☐ PlayStation 4

☐ Other

Name

Web client 1

Authorized JavaScript origins

Enter JavaScript origins here or redirect URIs below (or both)

Cannot contain a wildcard (http://\*.example.com) or a path (http://example.com/subdir).

http://www.example.com

Authorized redirect URIs

Must have a protocol. Cannot contain URL fragments or relative paths. Cannot be a public IP address.

https://localhost:8443/RMS/GDAuth/gdAuthFinish

Create Cancel



12. In the **Authorized redirect URIs** field, enter the RMS redirect URL in the following format: **https://[hostname]:[port]/RMS/GDAuth/gdAuthFinish**. You will receive the Client ID and Client Secret. This Client ID and Client Secret will be used in the RMS settings page.

## Configuring your Google Drive App

Perform the steps shown below to configure the Google Drive app to RMS.

**Note:** After the configuration, RMS will display files and folders present in the My Drive folder in Google Drive.

1. After your Google Drive app has been created, open **RMS** and select the **Service Providers > Available Providers**.
2. Under **Google Drive**, copy the **Client ID** and **Client Secret** values to the **App Key** and **App Secret** fields respectively.
3. Enter the redirect URL configured in the Google Developer Console in the **Redirect URL**. The format of the URL is

`https://<RMS Address>:<port number>`

**Note:** If your Rights Management Server user intends to access the Rights Management Server portal using a different URI than the one added here then after logging in to Rights Management Server the user would not be able to add their Google Drive repository for their Rights Management Server account. Therefore you must include the URI the user types to access the Rights Management Server portal in the above field. It is recommended you include all versions of the URI that your user types in order to access the Rights Management Server portal.

4. Click **SAVE**.



---

### Configuring Rights Management Server

This chapter describes configuration steps for integrating Rights Management Server with Microsoft OneDrive.

The configuration procedures are broken into the following sections:

- [Creating your OneDrive App for Rights Management Server](#)
- [Configuring your OneDrive App](#)

## Configuring Rights Management Server for Microsoft OneDrive

Using the Microsoft OneDrive repository in RMS, users can view, and download the files they need but cannot push or edit the files.

Before you can begin adding OneDrive repositories to Rights Management Server you must create your OneDrive app which will interface with Rights Management Server to ensure that access to the repository is granted.

**Note:** The steps indicated below need to be done only once per Rights Management Server deployment. You must perform these configuration steps in order to successfully add OneDrive repositories to your Rights Management Server.

## Creating your OneDrive App for Rights Management Server

1. Log in to <https://account.live.com/developers/applications/index>.
2. Type the OneDrive application name.
3. Select a language, accept the terms, and click **I accept**.

### Enable your application to use Microsoft accounts

This site will allow your web-based Android and iOS applications to authenticate users via Microsoft accounts.

If you want to register an application for Windows 8.1 or Windows Phone 8.1, go to the [Windows Store Dashboard](#) instead.

Provide the name of your application that users will see.

Application name\*  
RMS x

Use letters, digits, and underscores only; 129-character limit.

Language\*  
English (United States) ▼

Select your application's primary language.

Clicking **I accept** means that you agree to the Microsoft services [terms of use](#). Read [Privacy & Cookies](#).

**I accept** **Cancel**

#### 4. From the left menu, select **Settings > API Settings**.

RMS

Settings

- Basic Information
- API Settings**
- App Settings
- Localization

Mobile or desktop client app:  
☐ Yes ☒ No

Target domain:

Restrict JWT issuing:  
☒ Yes ☐ No

Root domain:

Redirect URLs:  
 [Add another redirect URL](#)

[Save](#) [Cancel](#)

Mobile client applications use a different OAuth 2.0 authentication flow. Selecting Yes will allow mobile clients to use this authentication flow. [Learn More](#)

This is the domain that other apps will use when they request a JWT for your app on Windows (such as www.contoso.com).

Limits the issuing of JSON Web Tokens (JWT) for your domain to exclusively this application.

All redirect URLs must fall within your root domain.

Specify the exact URL you will be redirecting users to (such as http://www.contoso.com/redirect). You must provide at least one redirect URL.

#### 5. Select **No** to create desktop client app.

#### 6. In the **Redirect URLs**, enter the RMS server address in the following format:

<Your Rights Management Server name>:<Port number>/RMS/ODAuth/odAuthFinish. For example, https://Seletar:8443/RMS/ODAuth/odAuthFinish.

#### 7. Click **Save**. You will receive the Client ID and Client secret in the **Settings > App Settings** page. This Client ID and Client secret will be used in the RMS settings configuration.

## Configuring your OneDrive App

Perform the steps shown below to configure the OneDrive app to RMS.

1. After your OneDrive app has been created, open **RMS** and select **Service Providers > Available Providers**.
2. Select **OneDrive > Configure**.
3. Under **OneDrive**, copy the **Client ID** and **Client Secret** values to the **App Key** and **App Secret** fields respectively.
4. Enter the redirect URL configured in the OneDrive Developer Console in the **OneDrive Redirect URL**. The format of the URL is

https://<RMS Address>:<port number>

**Note:** If your Rights Management Server user intends to access the Rights Management Server portal using a different URI than the one added here then after logging in to Rights Management Server the user would

not be able to add their Microsoft OneDrive repository for their Rights Management Server account. Therefore you must include the URI the user types to access the Rights Management Server portal in the above field. It is recommended you include all versions of the URI that your user types in order to access the Rights Management Server portal.

5. Click **SAVE**.

---

### Granting Rights to Users

NextLabs Rights Management Server assumes that all users must be granted rights to perform different actions (View, Print, etc.). For example, if you have not granted View rights for a document to a set of users, Rights Management Server denies them from viewing it.

*Note:* If you are upgrading from an RMS version prior to 8.1, you must revise your existing policies to ensure your users are granted the appropriate rights for each action they are authorized to perform.

Therefore, in NextLabs Policy Studio you must define Allow policies which grant specific rights to users. For more information on using Policy Studio, refer to the NextLabs Control Center documentation.

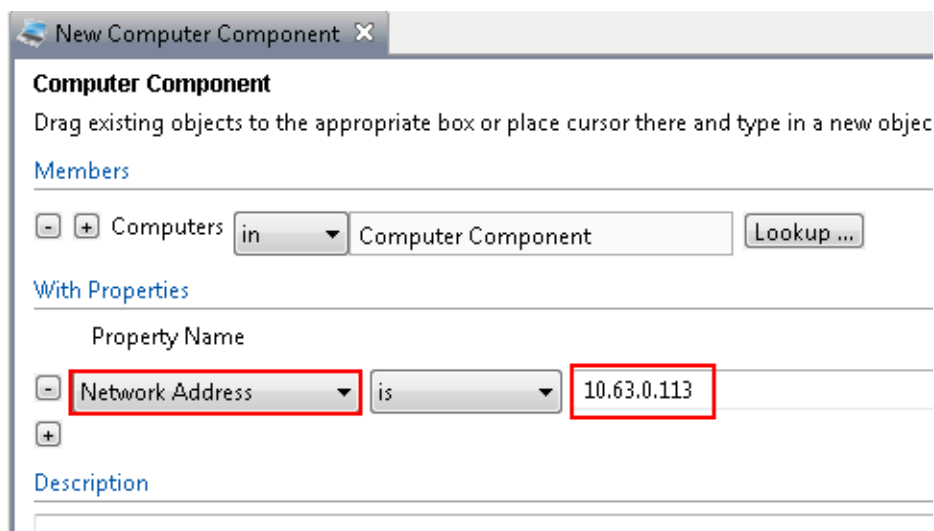
## Enforcing IP Address Policies

Rights Management Server enforces policies that are triggered based on the IP address specified for a Computer component in your policy.

For instance, if a policy denies the open action for a file based on the requesting computer's IP address, then Rights Management Server does not let the user view it.

The image below indicates the **Network Address** property name that is used to specify the IP address of your Computer component.

You can then use this Computer component in your respective policy.



The screenshot shows a window titled "New Computer Component". Inside, there's a section "Computer Component" with instructions: "Drag existing objects to the appropriate box or place cursor there and type in a new object". Below this are two sections: "Members" and "With Properties". In the "Members" section, there's a list with "Computers" and a "Lookup ..." button. In the "With Properties" section, there's a "Property Name" field. The dropdown menu is open, showing "Network Address" (highlighted with a red box). The operator is "is" and the value is "10.63.0.113" (also highlighted with a red box). There's a "+" button below the property list and a "Description" field at the bottom.

For more information about the NextLabs Policy Studio and defining policies for your particular deployment, refer to the NextLabs Control Center documentation.



## Enforcing Physical Location Policies

Rights Management Server enforces policies that are triggered based on the physical location specified for a User component in your policy.

*Note:* This feature is supported only for public IP addresses which adhere to the IPv4 standard.

For instance, if a policy denies the open action for a file based on the requesting computer's country code, then Rights Management Server does not let the user view it.

The image below indicates the `user_location_code` property name that is used to specify the country code of your User component.

*Note:* The country code that you specify in the policy must be ISO 3166-2 letter code.

You can then use this User component in your respective policy.

The screenshot shows the 'physical location' policy configuration in the NextLabs Policy Studio. Under the 'User Component' section, the 'Members' list contains 'Users' in a 'User Component'. The 'With Properties' section shows a property named 'user\_location\_code' (highlighted with a red box) set to 'is' (highlighted with a red box) with a value of 'CN' (highlighted with a red box). The 'Description' section is empty.

For more information about the NextLabs Policy Studio and defining policies for your particular deployment, refer to the NextLabs Control Center documentation.

## Inserting Hyperlinks in your Policy Obligation

Rights Management Server can handle hyperlinks specified as html code in the your policy obligation's Display User Alert field and embed it in your user alert message.

The html code can be inserted into the Display User Alert field of the Obligations section of your Policy (refer to the image below).

**Obligations:**

On Deny ☒ Log

☒ **Display User Alert**

For more information, click `<a href="http://www.companypolicies.com" target="_blank">`

☐ Send Email

☐ Custom Obligation

The following table lists the different kinds of hyperlinks you can specify in your policy obligation's display user alert field.

Hyperlink	Description
Mailing someone	<p>You can insert a hyperlink to trigger a compose mail form. For example, you can paste the following into the Display User Alert field:</p> <p>You need to request access for this document. If you want to email the Administrator, click <code>&lt;a href="mailto:someone@example.com"&gt; here&lt;/a&gt;</code></p>
Inserting a web address	<p>You can insert a hyperlink to redirect users to a relevant web address. For example, you can paste the following into the Display User Alert field:</p> <p>You are viewing a confidential document. For more information on handling such information, click <code>&lt;a href="http://www.companyinformationpolicy.com" target="_blank"&gt; here&lt;/a&gt;</code></p>

---

## Defining Application name in policies for RMS

RMS passes a set of attributes to Policy Controller for evaluating rules. If you are launching RMS directly, RMS will pass the **RMS** string to the Policy Controller. If you are launching RMS from the SharePoint app (SharePoint Online/Premise), RMS will pass the **RMS\_SHAREPOINT** string.



If you are defining a policy which includes a check for the application, make sure that you use the right string while defining the application component in policies.



### FAQs

The following is a list of frequently encountered situations and suggestions for how you can attempt to resolve them.

Question	Possible Answer
Why can't I access my Dropbox Repository via the Rights Management Server user interface?	You might have de-authorized the Dropbox app for Rights Management Server. Without the authorized Dropbox app, Rights Management Server cannot retrieve any information via your Dropbox links. You must remove the Dropbox repository links from Rights Management Server since they cannot be used anymore.
Why is my Rights Management Server User Interface displaying inconsistently?	Check your screen resolution. The recommended screen resolution for the Rights Management Server user interface is 1366 x 768. If you are using Internet Explorer 9 (IE9) to access the Rights Management Server UI, then you might have to switch off the compatibility view option. This feature in IE9 is meant to be used to view web pages that were designed for earlier versions of Internet Explorer. <b>NOTE:</b> You must also un-check the Display intranet sites in compatibility View.
Why can't I view a NXL protected document in my internal company SharePoint site in Rights Management Server?	- Your user account might not be authorized to view the NXL protected document in Rights Management Server. Contact your IT Administrator. - You might be logged in to the Rights Management Server portal as a User that is not authorized to view the document. You might need to logout of Rights Management Server and then log in again using the user credentials that are authorized to view your NXL protected document.
Why do I see the 403 (forbidden) message when attempting to access a NXL protected file that I have access to?	You might be using self signed certificates. To switch off this SharePoint requirement to use HTTPS when interacting with remote web apps, you must run some scripts. For more information, refer to this <a href="#">Microsoft MSDN article</a> .
Why do I see a Rights Management Server login screen when I select the <b>View in Rights Management Server</b> menu option in Microsoft SharePoint?	You can avoid being prompted for the Rights Management Server login screen each time you select the <b>View in Rights Management Server</b> in Microsoft SharePoint by adding both Microsoft SharePoint site and Rights Management Server as Trusted Sites in Internet Explorer.
Why can't I see NXL protected files listed in my SharePoint repository's search results in Rights Management Server?	If your NXL protected files are present in your SharePoint repository but are not displayed in the search results then you might need to wait until your SharePoint server completes the new crawl or you might need to request your SharePoint Administrator to initiate a preemptive crawl.

Question	Possible Answer
Why can't I pinch zoom when viewing NXL protected documents in a mobile device?	The pinch zoom gesture is disabled for NXL protected files that are viewed on a mobile device. You can instead use the zoom in  and zoom out  icons present on your screen.
Why can't I see my Microsoft SharePoint repository search results?	<p>If your Microsoft SharePoint repository contains more than 1,000 files, then in order to allow your users to view search results in Rights Management Server you must run the following management shell command on your SharePoint server:</p> <pre>\$ssa = Get-SPEnterpriseSearchServiceApplication \$ssa.MaxRowLimit = 10000 \$ssa.Update() iisreset</pre> <p>The above command allows you to set the maximum number of rows limit in SharePoint to 10,000 (rather than the default 1,000). This allows your Rights Management Server user to view the maximum number of matching results from their SharePoint repository.</p> <p><b>NOTE:</b> If your SharePoint repository has more than 10,000 files then you won't be able to view them in the search results page in Rights Management Server, since Microsoft SharePoint only permits a search query to retrieve a maximum of 10,000 files.</p>
Why can't I see a new feature in my Rights Management Server user interface?	You might need to clear your web browser's cache in order to view the latest Rights Management Server build.
Why can't I view an NXL document although I have the access rights?	<p>You might have configured the ICENet Server URL incorrectly during the installation. To update the ICENet Server URL, perform the following steps:</p> <ol style="list-style-type: none"> <li>1. Open the following configuration file: &lt;RMS_DATA_DIR&gt;\javapc\config\commprofile.xml.</li> <li>2. Edit the <b>DABSLocation</b> field with a proper ICENet Server URL. For example, https://my-icenet-server:8443/dabs.</li> <li>3. Restart the Rights Management Server.</li> </ol>
How do I decrypt bundle.bin in Embedded Java Policy Controller?	<ul style="list-style-type: none"> <li>- Embedded Java PC currently doesn't include the decrypt.bat utility that can be used to decrypt the policy bundle.</li> <li>- Copy the <b>decrypt.bat</b> and <b>decryptj</b> folders from any other Policy Controller installation to the &lt;RMS_DATA_DIR&gt;\javapc folder.</li> <li>- Ensure that you specify a valid JAVADIR in decrypt.bat. For example, you can specify: set JAVADIR="C:\Program Files\NextLabs\RMS\external\jre\bin"</li> </ul>
How do I change the port number used for Key Management after the RMS installation?	<ol style="list-style-type: none"> <li>1. Stop RMS.</li> <li>2. Specify the desired port number for the parameter <b>EMBEDDEDJPC_RMI_PORT_NUMBER</b> in the file &lt;RMS_DATA_DIR&gt;\RMSConfig.properties.</li> <li>3. Specify the same port number for the parameter <b>rmi_registry_port</b> in the file &lt;RMS_DATA_DIR&gt;\javapc\jsservice\config\KeyManagementService.properties.</li> <li>4. Start RMS.</li> </ol>

Question	Possible Answer
I get the following error "Error occurred while processing the file" while trying to view the CAD files in Linux OS.	<p>Check whether these files are present in the RMS server.</p> <ol style="list-style-type: none"> <li>1. /usr/lib64/libXext.so.6</li> <li>2. /usr/lib64/libXmu.so.6</li> <li>3. /usr/lib64/libGLU.so.1</li> </ol> <p>If these files are not present, then run the following commands to download and install</p> <pre>yum install libXext-1.3.3-3.el7.x86_64 yum install libXmu-1.1.2-2.el7.x86_64 yum install mesa-libGLU-9.0.0-4.el7.x86_64</pre>

## UI Display Problems

If your Rights Management Server login screen is displaying inconsistently in Internet Explorer, then you might need to check the Compatibility View settings of Internet Explorer or your monitor's screen resolution.



For more information, refer to [Accessing Rights Management Server using Internet Explorer](#) and [Minimum Screen Resolution](#).

## SSL Certificate Exceptions

If you are unable to access a NXL protected file via your SharePoint site in Rights Management Server, and your RMS.log file contains the following error:

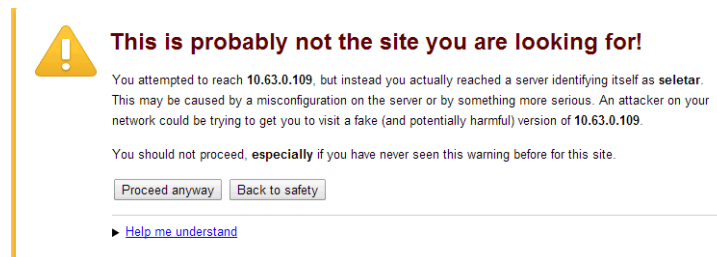
SSL Certificate Exception
org.apache.axis2.AxisFault: javax.net.ssl.SSLException: Connection has been shutdown: javax.net.ssl.SSLHandshakeException: sun.security.validator.ValidatorException:PKIX path building failed: sun.security.provider.certpath.SunCertificate

then you need to import your SSL certificate for SharePoint into your Rights Management Server TrustStore (which is specifically called cacerts).

For more information, refer to [Exporting a Self-Signed Certificate to Rights Management Server](#).

## Internet Protocol (IP) and Hostname Mismatch

If you are using self signed certificates for your Microsoft SharePoint - Rights Management Server deployment then while accessing your Microsoft SharePoint site or the NXL protected document in Rights Management Server (via your web browser) you might encounter the following SSL certificate warning:



This indicates that you attempted to access a machine using an IP address for which you did not have a security certificate imported to your web browser.

You must ensure that you have a consistent security certificates imported into the user's web browser (Trusted Root Certification Authorities) for any IP address, FQDN or hostname that your user will use to access SharePoint or Rights Management Server.

For more information, refer to [Importing a Self Signed Certificate for the User](#).

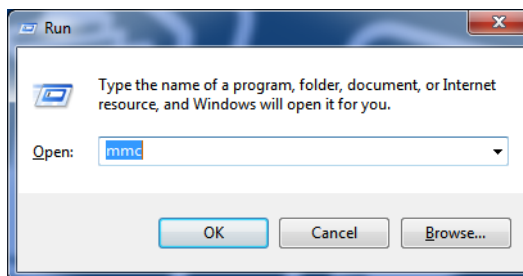
## Importing a Self Signed Certificate for the User

When deploying Rights Management Server for a demo environment you can use a self signed certificate to the user's web browser's Trusted Root Certificate Authority. This ensures that the user's web browser is able to successfully view a NXL protected file.

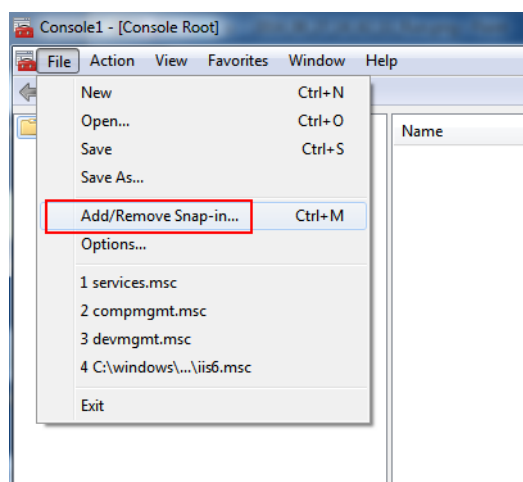
**Note:** For production environments you must use certificates issued by a Trusted Certificate Authority.



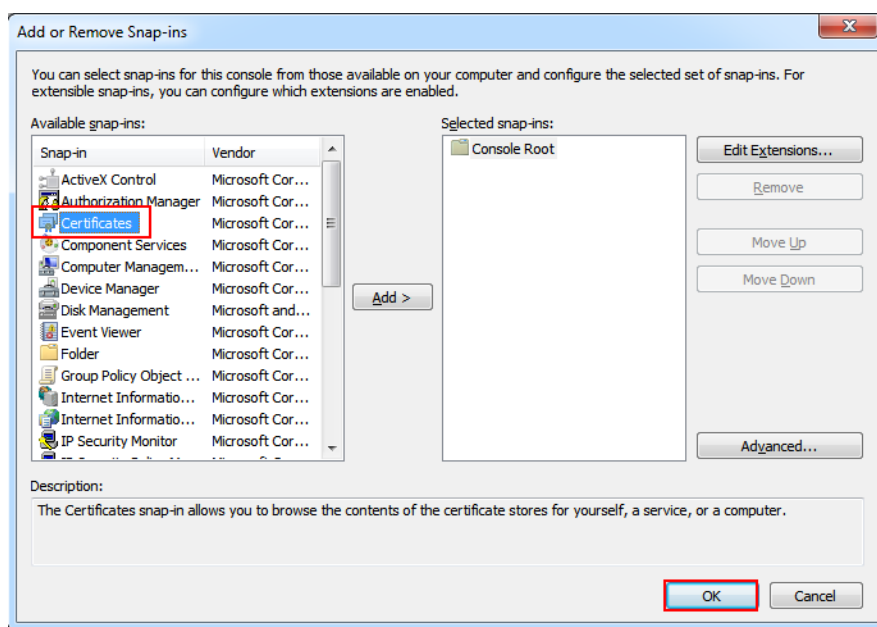
1. In your user's machine, navigate to **Start > Run** and type `mmc`.



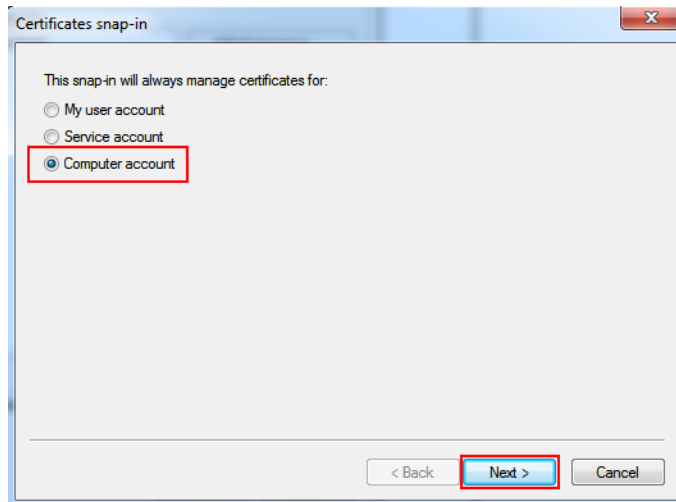
2. In the Microsoft Management Console, select **File > Add/Remove Snap-in**.



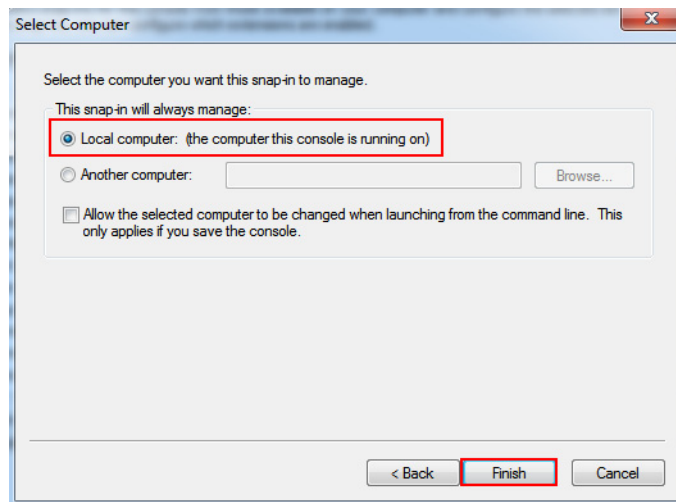
3. In the Available Snap-ins list select **Certificates** and click **OK**.



4. In the Certificate snap-in window, type select **Computer account** and click **Next**.

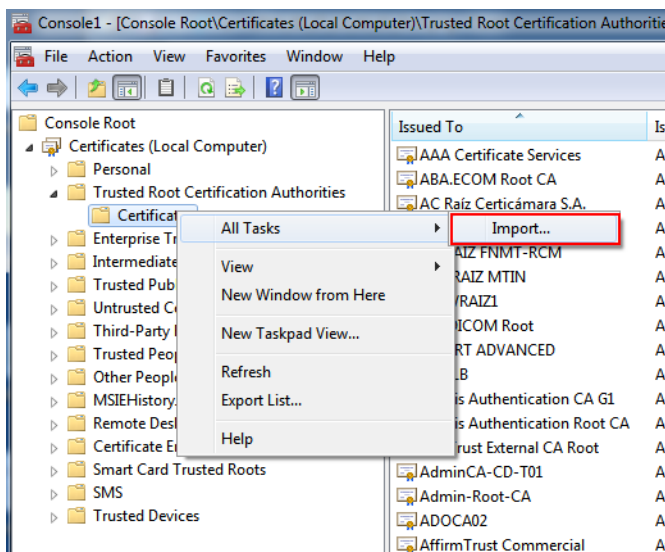


5. Select **Local Computer** and click **Finish**.

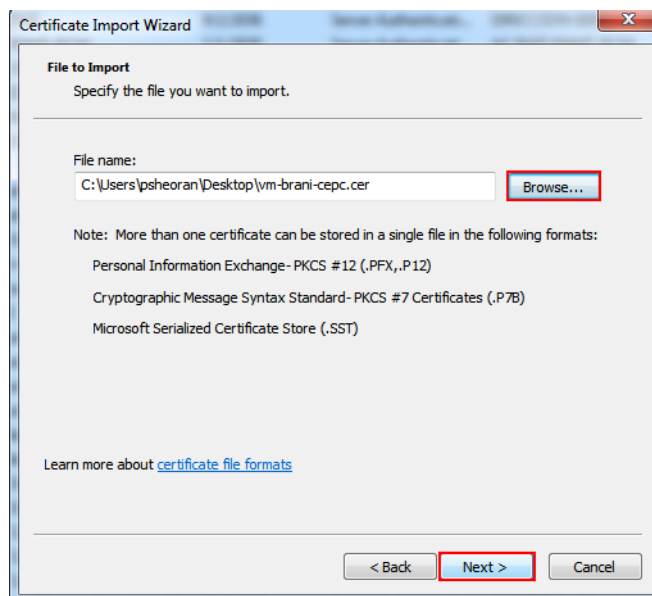


6. Navigate to **Certificates (Local Computer) > Trusted Root Authentication Authorities > Certificate** and right-click.

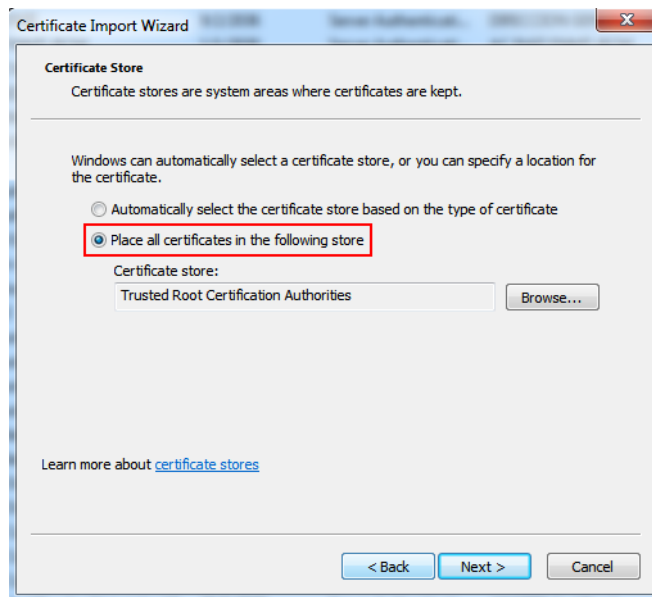
7. Select **All Tasks > Import**.



8. Click **Browse** to select your self signed security certificate and click **Next**.



9. Select **Place all certificates in the following store** and click **Browse** to select the **Trusted Root Certification Authorities**.



10. Click **Next**.

11. Click **Finish**.

