NEXTLABS®

Rights Management Server

Administrator’s Guide

Release 8.2

November 2015

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

TRADEMARKS

NextLabs®, ACPL®, RMS™, 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
info@nextlabs.com
650.577.9101

Document Revision Number: RMS-8.2

NEXTLABS®

Contents

1. Introduction 7

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

2. Installing Rights Management Server 15

Installing Rights Management Server 15

Before You Start. 16
Prerequisites 16
Supported Platforms 16
Software 16
Supported Web Browsers 16
Supported File Formats. 17
Database for Location lookup 18

Installing Rights Management Server 19
License Key File 19
Running the Installation Wizard. 19
Running a Silent Installation 23
Logging in to the Rights Management Server Portal. 25
Minimum Screen Resolution 25
Accessing Rights Management Server using Internet Explorer 25

Uninstalling Rights Management Server 29

Running the Uninstallation Wizard 29
Performing a silent Uninstallation 29

Upgrading Rights Management Server from 8.0/8.1 to 8.2 31

Starting/Stopping/Restarting RMS Service 32

3. Configuring Rights Management Server 33

Configuring Rights Management Server 33

Integrating with SharePoint Online 34
Registering your SharePoint Online Application 34
Creating your SharePoint Online App 36
Deploying your SharePoint Online App 36

Integrating with SharePoint
On-Premise 37
Deploying the Provider Hosted App 37
Prerequisites 37
Registering the High-Trust App 38
Creating your SharePoint On-Premise Apps 38
Configure the Remote Web Server with the Certificate 38
Importing the .pfx Certificate 39
Importing the .cer Certificate 39
Configuring SharePoint to Use the Certificate 40
Distributing the .cer file to SharePoint 40
Configuring the Certificate 40
Modifying the web.config File 41
Publishing Remote Web App in SharePoint 41
Configuring Protocol Binding for the Web Application 41
Configuring Authentication for the Web Application 42

Configuring your Java Policy Controller 43

Configuring Remote Java Policy Controller Communication 44
KeyStore & TrustStore Files 44
Generating the Certificate 45
Exporting the Certificate 46
Importing the Certificate into the TrustStore 46
Adding Attributes to the KeyManagement Services File 46
. . . . 48

Configuring a NXL Filter for MS SharePoint 49
Specifying the NXL File Type 49
Specifying NXL Registry Entries 49

Configuring Alternate Access Mapping 51
Configuring Alternate Access Mappings in Sharepoint 2010 and 2013 51

Configuring Logging 53

Configuring the Remote Policy Controller Settings 54

Configuring the Mail Server Settings 56

Configuring Client Management Settings. 58

Configuring User Location Settings 59

Other Configuration Parameters 60

Configuring Watermark Information 61
- Policy based Watermark 61
  - Config File based Watermark 64
  - Policy versus Config File based Watermark 65
- Configuring the Session Timeout Duration 66

Configuring Rights for Control Center 67

Configuring Rights Management Obligation. 68

Configuring the Rights Management Client 69
- Specifying the RMC package location 69
- Downloading the Rights Management Client. 69
- Configuring RMC_Classification.xml 69
- Configuring Local or External Login Credentials for RMC 69

Configuring RMS Memory Settings 71

Importing Your Own SSL Certificates for Rights Management Server. 72

4. Repositories 73

Adding a Repository. 73

Integrating with SharePoint 75

Exporting a Self-Signed Certificate to Rights Management Server 76

5. Integrating with SharePoint Online 81

Introduction. 81

Registering your SharePoint Online App 82

Creating your SharePoint Online App 84
- Deploying your SharePoint Online App 85

Removing an Expired Client Id and Certificate Name 86

6. Integrating with SharePoint On-Premise 87

Introduction. 87

Deploying the Provider Hosted App 89
- Prerequisites 89
- Registering the High-Trust App 89
- Configure the Remote Web Server with the Certificate .89
  - Importing the .pfx Certificate 90
  - Importing the .cer Certificate 90
- Configuring SharePoint to Use the Certificate 91

Distributing the .cer file to SharePoint 91

Configuring the Certificate. 91

Modifying the SetParameters File 92

Modifying your Web Server’s web.config File 93

Publishing Remote Web App in SharePoint 93

Configuring Protocol Binding for the Web App 94

Configuring Authentication for the Web App 94

Creating your SharePoint On-Premise Apps 95

7. Integrating with Dropbox 97

Configuring Rights Management Server 97

Configuring Rights Management Server for Dropbox Repositories 98

Creating your Dropbox App for Rights Management Server 98

Configuring your Dropbox App. 100

Applying for Production Status. 101

8. Access Control using Policies 103

Granting Rights to Users 103

Enforcing IP Address Policies 104

Enforcing Physical Location Policies 105

Inserting Hyperlinks in your Policy Obligation 106

9. Troubleshooting 107

FAQs 107

UI Display Problems 109

SSL Certificate Exceptions 109

Internet Protocol (IP) and Hostname Mismatch. 109

Importing a Self Signed Certificate for the User. 110

1 Introduction

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.
- Troubleshooting contains a FAQ list 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>`	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 `<RMS_DATA_DIR>` are: • Windows Deployment: `C:\ProgramData\NextLabs\RMS\datafiles` • Linux Deployment: `/var/opt/nextlabs/RMS/datafiles` The Rights Management Server Data Directory contains files like config file, log file, etc. The `RMSConfig.properties` file contains details about the Active Directory. **NOTE:** 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.
`<RMS_INSTALL_DIR>`	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 `<RMS_INSTALL_DIR>` are: • Windows Deployment: `C:\Program Files\NextLabs\RMS\` • Linux Deployment: `/opt/nextlabs/RMS/`

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.

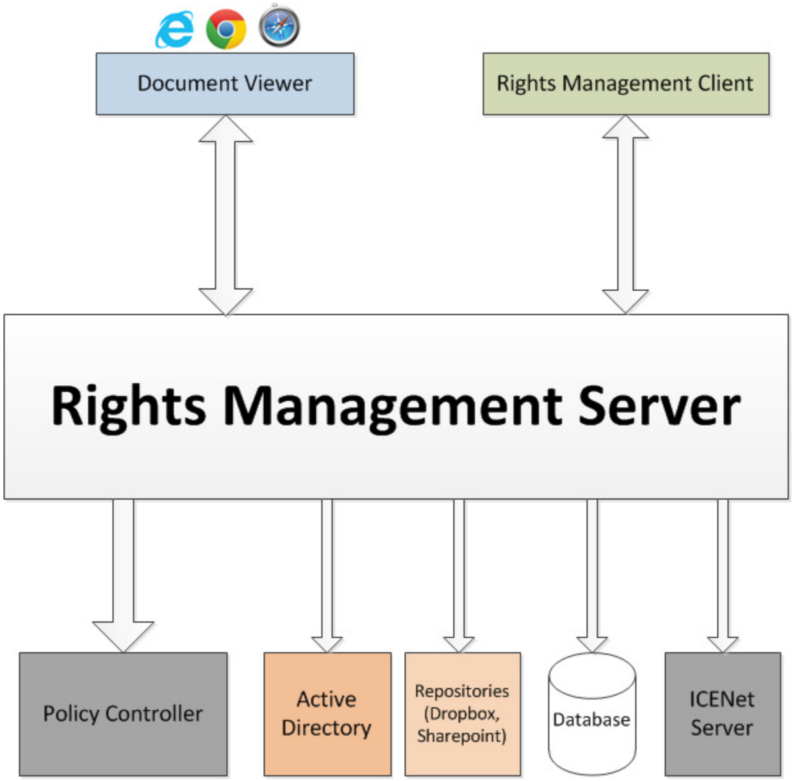
Rights Management Server communicates with the NextLabs Rights Management Client (RMC) to:

- 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

2 Installing Rights Management Server

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 8.2
- 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 6.5 and 7

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 Web Browsers

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

- Internet Explorer (Version 9, 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 9, 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

- doc and docx
- ppt and pptx

Note: PowerPoint slides that contain Smart Art created prior to Microsoft Office 2007 Service Pack 2 are not supported.

- xls and xlsx
- pdf
- dwg

Note: For Windows OS, the dwg file will be displayed in a 3d viewer. For Linux, it will be displayed in a 2d viewer.

- txt
- png and jpg
- jt and prt

Note: 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 Configuring Rights for Control Center. Watermarks are not supported for rh files.

- SAP
  - rh
  - vds
- Common
  - igs
  - stp
  - stl
  - step
- eDrawings 2015
  - sldprt
  - sldasm
  - prt
- Solid Edge
  - par
  - psm
  - asm (See the Note on page 18)

- Catia V5
  - cgr
  - CATPart
  - CATProduct (See the Note on page 18)
- 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.

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.

License Key File

To view the SAP 3D (VDS and RH) and CAD files, 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:

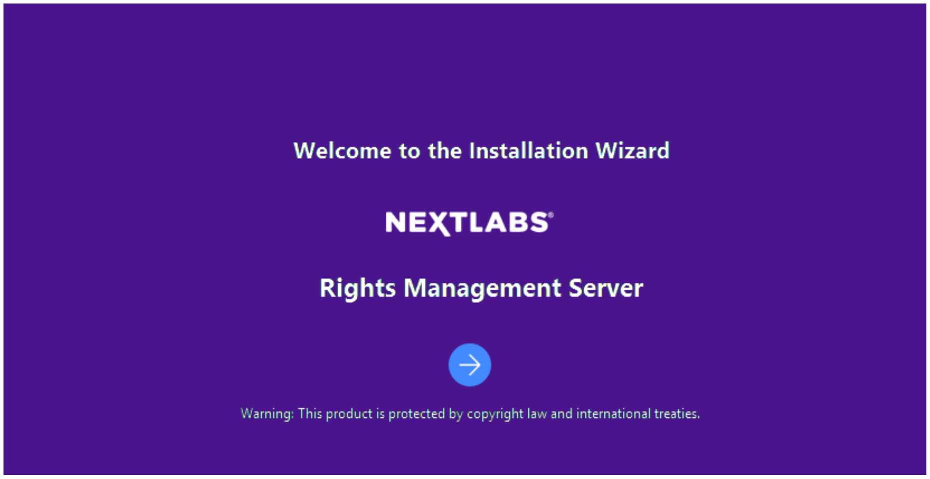
   - On a Windows server, you can launch the installer from one of the following methods:
     - launch the command prompt as an Administrator.
     - In the command prompt, navigate to the folder that contains **install.bat**.
     - From this directory, run the following command:`install.bat`

       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).



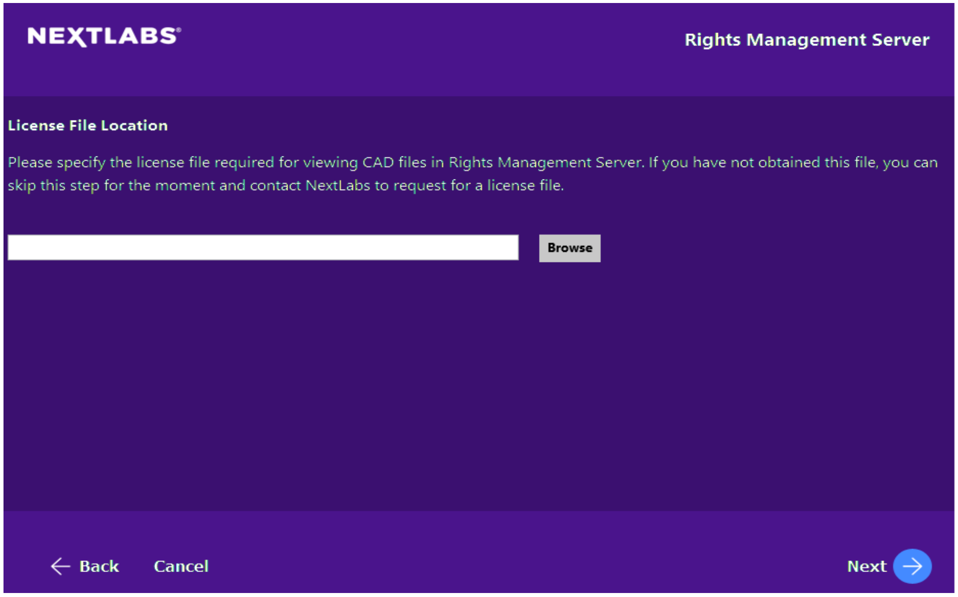
Welcome to the Installation Wizard

Rights Management Server

Warning: This product is protected by copyright law and international treaties.

4. On the License Agreement screen, click **Agree and Proceed**.

5. Specify the location of the **license.dat** file and click **Next**. Skip this step if you do not have a license to view the SAP or CAD files.

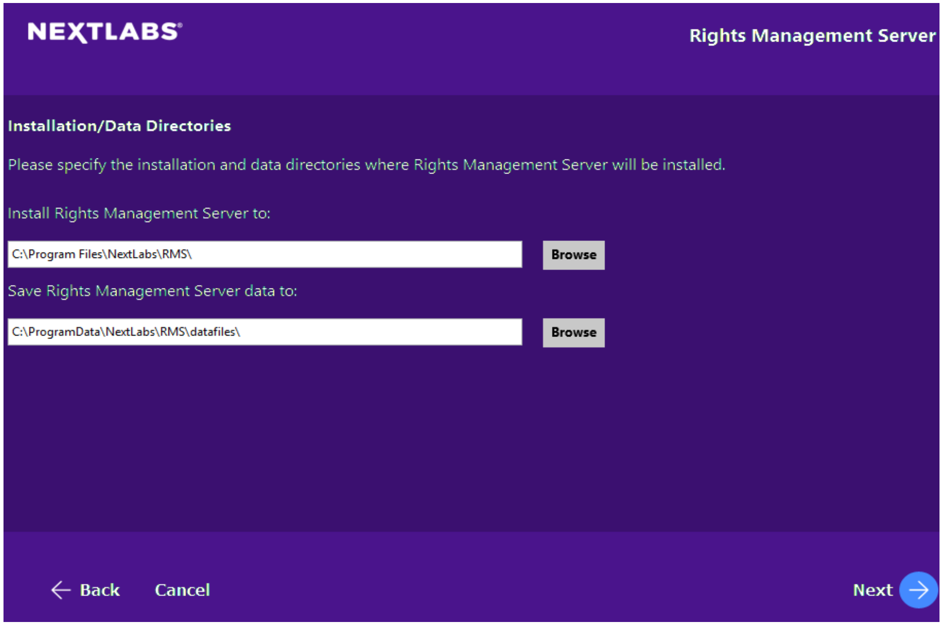


License File Location

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.

6. 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.



Installation/Data Directories

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

Install Rights Management Server to: C:\Program Files\NextLabs\RMS\

Save Rights Management Server data to: C:\ProgramData\NextLabs\RMS\datafiles\

7. 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 for RMS**: Enter the port number to access RMS using HTTPS. The default port number is 8443.
   - **Shutdown port for RMS:** Enter the shut down port that will be used by RMS. The default port number is 8005.
   - **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.

8. Configure the Active Directory. NextLabs Rights Management Server integrates with Microsoft Active Directory (AD) and uses it to authorize users.

   - **Server Host Name** - The name of your AD server. For example, MyADServerName.
   - **Domain Name** - The name of the domain your AD server is on. For example, mydomain.companydomain.com
   - **Search Base** - The location in your AD 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 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.

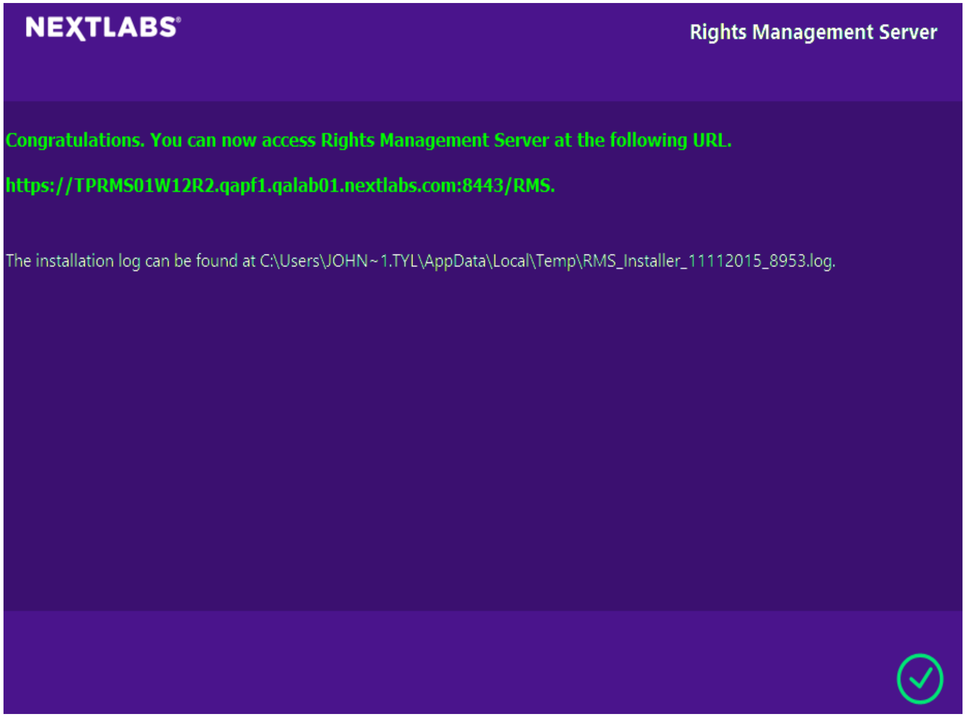
9. Enter the IP Address or the fully qualified domain name (FQDN) of the ICENet Server in the following format: **https://<ICENet-server-name>:<portnumber>.** For example: **https://myICENetServer:9191.**

   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 58) for details.

10. Click **Next** to begin installation. You will receive a notification when the installation is complete.

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



Congratulations. You can now access Rights Management Server at the following URL.

https://TPRMS01W12R2.qapf1.qalab01.nextlabs.com:8443/RMS.

The installation log can be found at C:\Users\JOHN~1.TYL\AppData\Local\Temp\RMS_Installer_11112015_8953.log.

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

12. 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 71) 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 SAP and CAD 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. Rights Management Server integrates with Microsoft Active Directory (AD) and uses it to authorize users.
    - **ldap_host_name** - Enter the name of your AD server. For example, MyADServerName.
    - **ldap_domain** - Enter the name of the domain your AD server is on. For example, mydomain.companydomain.com.
    - **ldap_search_base** - Enter the location in your AD 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.

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 71) 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 **Sign 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.

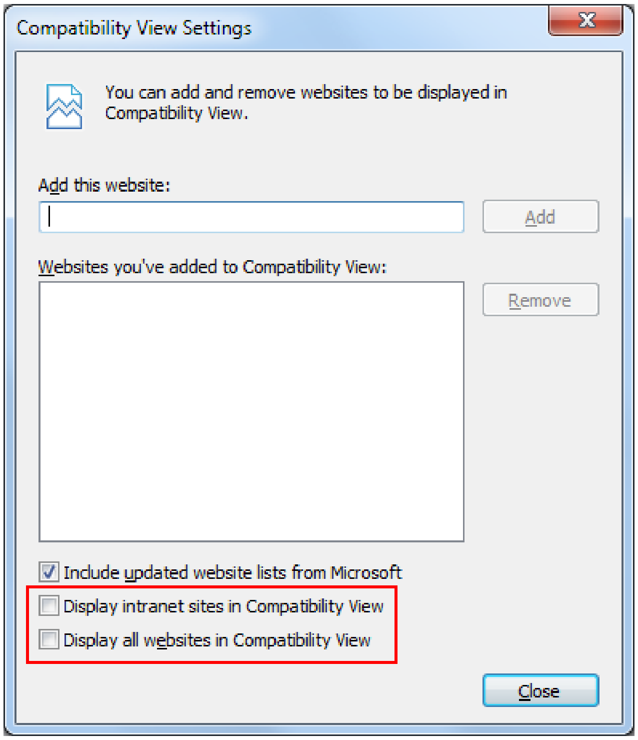
Compatibility View Settings

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:



Compatibility View Settings
Add this website:
Add
Websites you've added to Compatibility View:
Remove
Close

You can add and remove websites to be displayed in Compatibility View.

☑ Include updated website lists from Microsoft

□ Display intranet sites in Compatibility View

□ Display all websites in Compatibility View

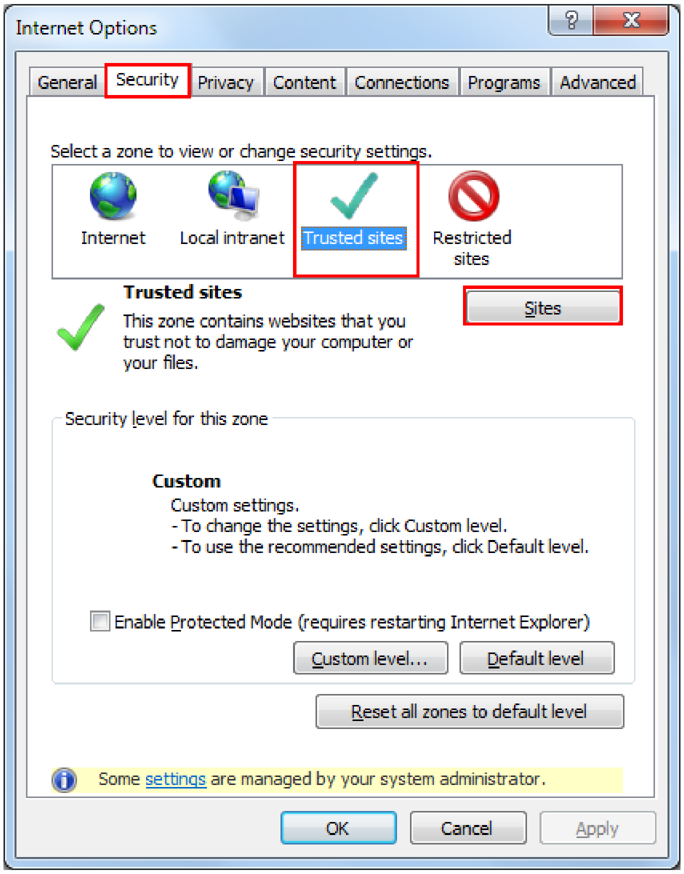
- **Display Intranet sites in Compatibility View**
- **Display all websites in Compatibility View**

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**.



Select a zone to view or change security settings.

Trusted sites

This zone contains websites that you trust not to damage your computer or your files.

Security level for this zone

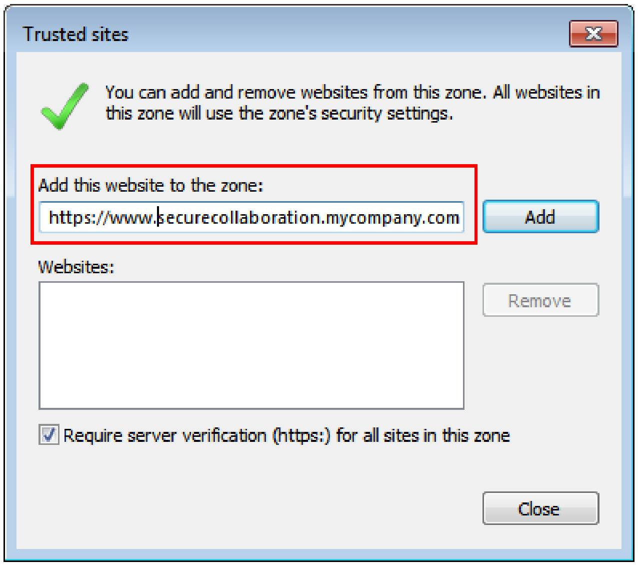
Custom

Custom settings.
- To change the settings, click Custom level.
- To use the recommended settings, click Default level.

☐ Enable Protected Mode (requires restarting Internet Explorer)

Some settings are managed by your system administrator.

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



You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:
https://www.securecollaboration.mycompany.com

Websites:

☑ Require server verification (https:) for all sites in this zone

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.

Running the Uninstallation Wizard

- On a Windows server
  - launch the command prompt as an Administrator.
  - In the command prompt, navigate to the **<RMS_INSTALL_DIR>/bin** 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>/bin** that contains **uninstall.sh**.
  - From this directory, run the following command as root: `bin/uninstall.sh` and follow the instructions.

Performing a silent Uninstallation

To uninstall the RMS server components using the silent 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 uninstallation values. This file is located in the installation directory where the **uninstall** script is present. You can edit the json file using a text editor.
3. Update the **delete_data_dir** field to **Yes** or **True**. The default value is **False** or **No**. When this field is set to Yes or True, the uninstaller will delete the data directory. The installation directory will always be deleted during uninstallation.
4. Run the uninstaller 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 uninstaller in the silent mode: `uninstall.bat -s`
- On a Linux server
  - navigate to the extracted folder.
  - From this directory, type the following command to run the uninstaller in the silent mode: `./uninstall.sh -s`

Upgrading Rights Management Server from 8.0/ 8.1 to 8.2

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 19) 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 SAP 3D (VDS and RH) and CAD files, 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 33) 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.

3 Configuring Rights Management Server

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:

- Integrating with SharePoint Online
- 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

Integrating with SharePoint Online

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 Application which handles all file access requests for any encrypted 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.

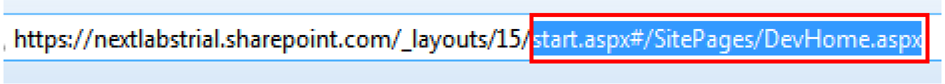
Currently Rights Management Server is only supported to work with Microsoft SharePoint Online and SharePoint 2013. You can create your SharePoint Online Application in Rights Management Server, but you need to register your SharePoint Online Application first.

Registering your SharePoint Online Application

Before you can use Rights Management Server to create your SharePoint Online Application you must register your SharePoint Online Application. 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.

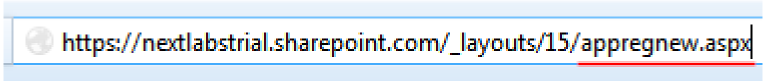
> *Note:* The following steps are applicable if you want to register a High-Trust App for SharePoint Online as well.

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 `layout/15/` as indicated below:



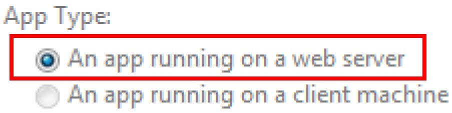
https://nextlabstrial.sharepoint.com/_layouts/15/start.aspx#/SitePages/DevHome.aspx

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.

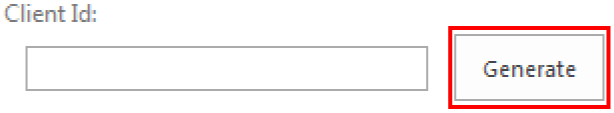


App Type:

● An app running on a web server

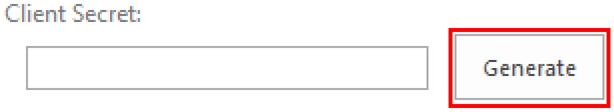
○ An app running on a client machine

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



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.



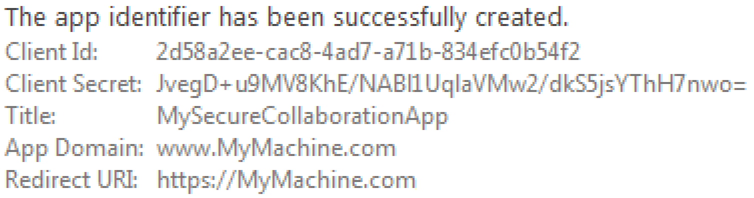
Note: If you are registering a High-Trust app then the **Client Secret** is not used but is still a mandatory value that must be generated for app registration.

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 Server, for example 10.168.23.28 or www.MyMachine.com** **NOTE:** 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**
Redirect URI	Publicly listed IP address or web address for your Rights Management Server Server with the appropriate protocol included, for example https://10.168.23.28/SC or https://MyMachine.com/SC

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/NABl1UqlaVMw2/dkS5jsYThH7nwo=
Title:	MySecureCollaborationApp
App Domain:	www.MyMachine.com
Redirect URI:	https://MyMachine.com

Creating your SharePoint Online App

1. Login to the Rights Management Server Administrator console.
2. Click the ⚙ icon.
3. Click **Application Settings**.
4. Click **SharePoint App Settings**.
5. Click **Add SharePoint Application**.
6. Select the **SharePoint Type** as **SharePoint Online**.
7. Type the following details:

Field	Description
Display Name	This is the displayed name of the SharePoint App you want to configure.
App Client Id	This is the **Client Id** value that was generated during the SharePoint Online app registration. For more details, see Registering your SharePoint Online Application.
App Client Secret	This is the Client Secret of the SharePoint App that you want to configure.

8. Click the download icon for your SharePoint Online App ⬇.

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

9. 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 ot a SharePoint 2013 site***.

This SharePoint Online App allows you to view your SharePoint Online encrypted files (.nxl) in the Rights Management Server Server.

Integrating with SharePoint On-Premise

SharePoint On-Premise refers to the stand alone deployment of SharePoint in your network. You can deploy a Rights Management Server-SharePoint On-Premise Applications to integrate the ability to view encrypted files via Rights Management Server. There are two applications that are created by Rights Management Server for deployment on SharePoint On-Premise:

- SharePoint On-Premise Application:
  This application 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 application.
- SharePoint On-Premise Web Application:
  This web application acts as a information broker between your Internet Information Service (IIS) and the SharePoint On-Premise Application.

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.

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 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
- A X.509 digital certificate for the remote web application 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 Application. You must perform these steps for your High-Trust App to register it before you move to the next section.

Creating your SharePoint On-Premise Apps

1. Login to the Rights Management Server Administrator console.
2. Click the ⚙ icon.
3. Click **Application Settings**.
4. Click **SharePoint App Settings**.
5. Click **Add SharePoint Application**.
6. Select the **SharePoint Type** as **SharePoint On-Premise**.
7. Type the following details:

Field	Description
Display Name	This is the displayed name of the SharePoint App you want to configure.
App Client Id	This is the **Client Id** value that was generated during the SharePoint Online app registration. For more details, see Registering your SharePoint Online Application.
App Client Secret	This is the Client Secret of the SharePoint App that you want to configure.

8. Click the download icon for your SharePoint On-Premise Apps ⤓.

Note: The SharePoint On-Premise Apps are downloaded as a zip file.

9. Extract your zip file. It contains two apps for your SharePoint On-Premise deployment.

Note: One of the apps is a SharePoint web application that must be deployed on your IIS. For more information about deploying it to your IIS refer to the sections below. The second is a 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.

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 app.

Importing the .pfx Certificate

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

Note: By default, IIS assigns a user called **ApplicationPoolIdentity** to its web applications 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 application, 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**.

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 application 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 the zip file in the <place holder for powershell script file location and names>

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 serveres 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 web.config File

The `web.config` file of your remote web application needs to be modified to contain new values for the following keys in the appSettings node:

Field	Description
ClientID	This is the **Client Id** value that was generated during the app registration. For more details, see Registering your SharePoint Online Application.
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

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 an example section that is inserted into the web.config file:

```
<appSettings>
  <add key="ClientID" value="c1c12d4c-4900-43c2-8b89-c05725e0ba30" />
  <add key="ClientSigningCertificatePath" value=" C:\MyCerts\MyCert.pfx" />
  <add key="ClientSigningCertificatePassword" value="mypassword6392" />
  <add key="IssuerId" value=" c1c12d4c-4900-43c2-8b89-c05725e0ba30" />
</appSettings>
```

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

Publishing Remote Web App in SharePoint

1. Copy all the files in RemoteWebApplicationPack to a folder on the remote server.

2. In this folder, open the `project_name.deploy-readme.txt` file, and follow the instructions in the file to install the web application using the project_name.deploy.cmd file.

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

Configuring Protocol Binding for the Web Application

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

Note: If the new web application 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 Application

When a new web application 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 application 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 application is designed to use and click **Enable** in the Actions pane.

Note: The web application 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:

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**.

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=sa1f78f49e437288039751654ece96ede

keypass=sa1f78f49e437288039751654ece96ede
```

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:

```
sa1f78f49e437288039751654ece96ede
```

3. Restart your Java Policy Controller.
4. In the Rights Management Server, click the ⚙ icon.
5. Select **Application Settings** and click **Policy Controller Settings**.
6. Specify the **KeyStore File** and **TrustStore File** locations and passwords in the following fields:

Rights Management Server Settings Field	Description
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. **NOTE:** 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 **NOTE: Specify the plain text (unencrypted) passwords in Rights Management Server.**
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 **NOTE: Specify the plain text (unencrypted) passwords in Rights Management Server.**

7. 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\.nxl
   ```

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**.

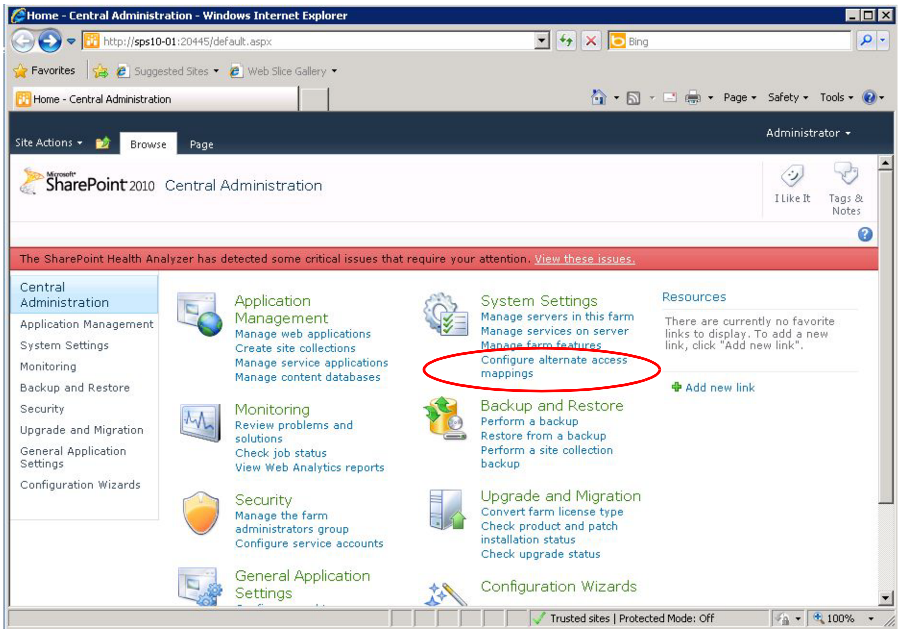
Configuring Alternate Access Mapping

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.

Configuring Alternate Access Mappings in Sharepoint 2010 and 2013

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.**

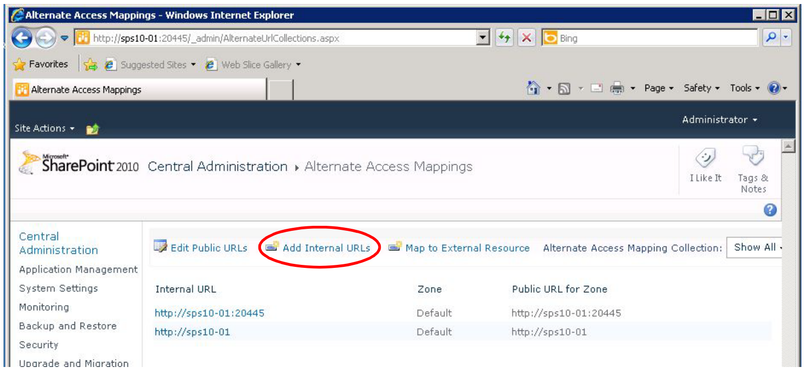

Home - Central Administration - Windows Internet Explorer
http://sps10-01:20445/default.aspx
Bing
Favorites
Suggested Sites
Web Slice Gallery
Home - Central Administration
Page
Safety
Tools
Site Actions
Browse
Page
Administrator
SharePoint 2010 Central Administration
I Like It
Tags & Notes
Central Administration
Application Management
System Settings
Monitoring
Backup and Restore
Security
Upgrade and Migration
General Application Settings
Configuration Wizards
Application Management
Manage web applications
Create site collections
Manage service applications
Manage content databases
System Settings
Manage servers in this farm
Manage services on server
Manage farm features
Configure alternate access mappings
Resources
Add new link
Monitoring
Review problems and solutions
Check job status
View Web Analytics reports
Backup and Restore
Perform a backup
Restore from a backup
Perform a site collection backup
Security
Manage the farm administrators group
Configure service accounts
Upgrade and Migration
Convert farm license type
Check product and patch installation status
Check upgrade status
General Application Settings
Configuration Wizards
Trusted sites | Protected Mode: Off
100%

The SharePoint Health Analyzer has detected some critical issues that require your attention. View these issues.

There are currently no favorite links to display. To add a new link, click "Add new link".

Figure 3-1: Alternate Access Mappings

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



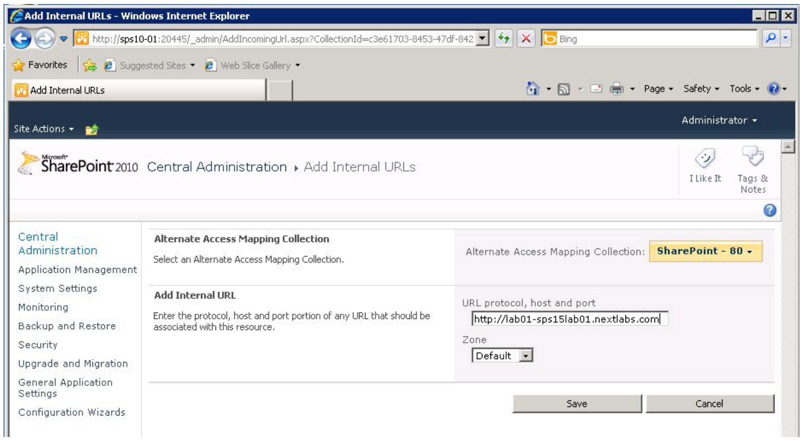
Internal URL	Zone	Public URL for Zone
http://sps10-01:20445	Default	http://sps10-01:20445
http://sps10-01	Default	http://sps10-01

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.



Alternate Access Mapping Collection

Select an Alternate Access Mapping Collection.

Alternate Access Mapping Collection: SharePoint - 80

Add Internal URL

Enter the protocol, host and port portion of any URL that should be associated with this resource.

URL protocol, host and port: http://lab01-sps15lab01.nextlabs.com

Zone: Default

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
`rootLogger`	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). **NOTE:** 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.
`MaxBackupIndex`	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.
`MaxFileSize`	this value determines the size of each log file. You must specifiy 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 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. Login to the Rights Management Server Portal.
2. Click the ⚙ icon.
3. Click **Application Settings**.
4. Click **Policy Controller Settings**.
5. In the Policy Controller Settings section, type the following details:

Field	Description
Enable Remote PC	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, select **Yes**. The default value is **No**. If the remote Java Policy Controller is selected 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:
	`https://<server name>:<port number>`
	For example:
	`https://RightsManagement.mycompany.com:8443`
	NOTE: 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	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. **NOTE:** 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.

Field	Description
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

6. Click **Test Connection** to verify that Rights Management Server can connect to the Policy Controller.

7. 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 the ⚙ icon.
3. Click **Application Settings**.
4. Click **Mail Server Settings**.
5. In the Mail Server Settings section, click **Yes** for **Allow Registration Request**.

Note: If this option is set to **No**, 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.

6. Type the following details:

Field	Description
Allow Registration Request	This is the option to allow new account requests via the Rights Management Server login page. Setting this value to No removes the **Request an account** hyperlink from the login page.
SMTP Host	This is the hostname of your SMTP Mail Server **NOTE:** If your Rights Management Server is deployed on a Linux system then you must specify the corresponding IP Address for this field.
SMTP Port	This is the port number at which Rights Management Server and SMTP communication occurs.
SMTP Authentication needed?	If you want to enable SMTP authentication prior to any email being sent due to Rights Management Server, then select **true**
SMTP User Name	This is the user name for the mail account which will send emails to the Administrator and sponsor on behalf of Rights Management Server.
SMTP Password	This is the password for the SMTP User Name

Field	Description
Reenter SMTP Password	Confirm your SMTP Password
SMTP Enable TLS	Transport Layer Security (TLS) is a protocol that encrypts and delivers messages in a secure fashion. If you want to use this protocol for communication between the Rights Management Server and your SMTP mail server then select **True**.
Email Subject	This is the subject of the email that the SMTP mail server sends on behalf of Rights Management Server. You can specify this to be something meaningful that would indicate the purpose of the email to be related to Rights Management Server user account creation.
Rights Management Server Administrator Email	This is the email address of the Administrator that you want to send the user account creation request email to.

7. 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 the ⚙ icon.
2. Click **Application Settings**.
3. Click **Client Management Settings**.
4. Type 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 **Client Version Number** 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.

5. 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 the ⚙ icon.
2. Click **Application Settings**.
3. Click **General Settings**.
4. Set the **Turn on User Location** option to **Yes**.
5. Type 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 identified time	This displays the last time the Location database file was updated. **NOTE:** 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 Database for Location lookup.
Location Update Frequency	This is the frequency of updates performed for the Location database file.

6. 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>

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

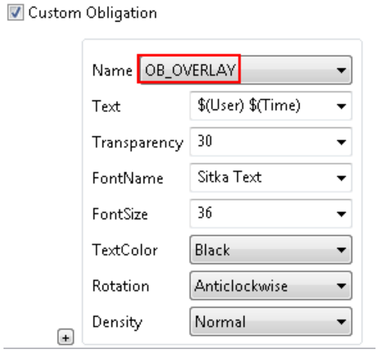
XML code for configuration.xml (Continued..)

```
<!-- 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

Name: OB_OVERLAY
Text: $(User) $(Time)
Transparency: 30
FontName: Sitka Text
FontSize: 36
TextColor: Black
Rotation: Anticlockwise
Density: Normal

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 **Black**.
Rotation	Select the direction of rotation for your watermark. The default value is **Anticlockwise**.
Density	Select how dense you want the displayed watermark to be. The default value is **Normal**. If you want to increase the density of the watermark displayed on your NXL protected documents, you can set this value to **Dense**. **NOTE:** This field of the custom obligation is only handled by Rights Management Server. If your policy is enforced my 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	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 RMSConfig.properties file. 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: yyyy-MM-dd This date format can also be any supported date and time pattern supported by java, as listed at this web link. The default value is: EEE MMM dd HH:mm:ss yyyy The above default value displays the following sample value: Wed Oct 16 00:00:00 2013 **NOTE:** If you specify the incorrect date format then this will display the default value format indicated above.
WATERMARK_FONT_SIZE	Set the value of this parameter to specify the font size of your watermark. The font size is in pixels. The default value is 36.
WATERMARK_FONT_COLOR	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. The default value is Black.
WATERMARK_FONT_TRANSPARENCY	Set the transparency level percentage of your watermark. You can specify a value between 0(fully opaque) and 100 (invisible). The default value is 30.
WATERMARK_ROTATION	Set the rotation direction of your watermark. You can specify the value as either Clockwise or Anticlockwise. The default value is Anticlockwise.
WATERMARK_DENSITY	Set the density of your watermark. you can specify the value as either Normal or Dense.

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 the ⚙ icon.
3. Click **Application Settings**.
4. Click **General Settings**.
5. In the General Settings section, type the number of minutes in the **Session Timeout** field.
6. Click **Save**.

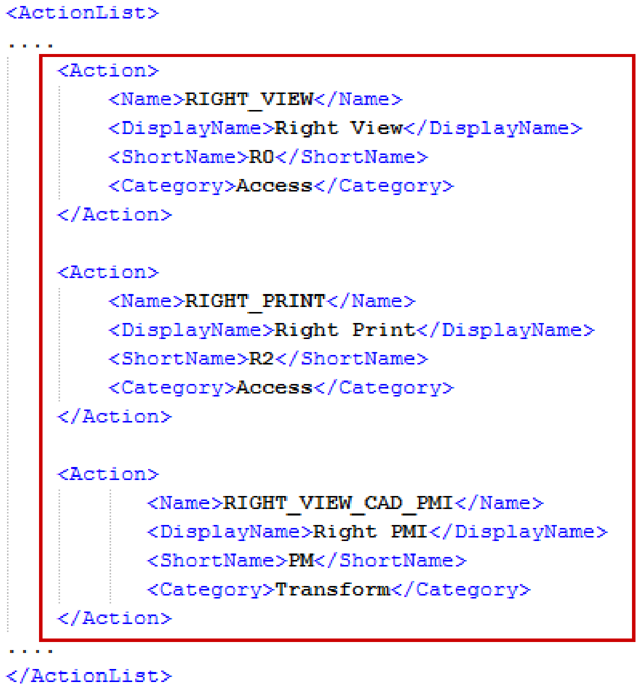
Configuring Rights for Control Center

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>RO</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. Login to the Rights Management Server Administrator console.
2. Click the ⚙ icon and select **Download Rights Management Client.**
3. In the new window, click **Download Rights Management Client** to download the installation package.

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.

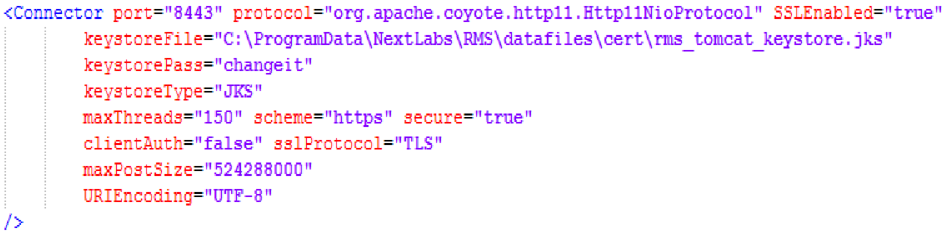
Configuring RMS Memory Settings

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 -Xmx256M”** 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.

4 Repositories

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 and Dropbox (for more information, refer to Configuring Rights Management Server for Dropbox Repositories) 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. Login to the Rights Management Server Administrator console.
2. Click the ⚙ icon.
3. Click **Manage Repositories**.
4. Click **Add Repository.**
5. 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. **NOTE:** 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 Configuring a NXL Filter for MS SharePoint.
Dropbox	If your files reside in Dropbox, select this option. **NOTE:** 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 Configuring Rights Management Server for Dropbox Repositories.

6. 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. Fore 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.

7. If you selected **Dropbox**, then type the **Repository Name**.

8. 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.

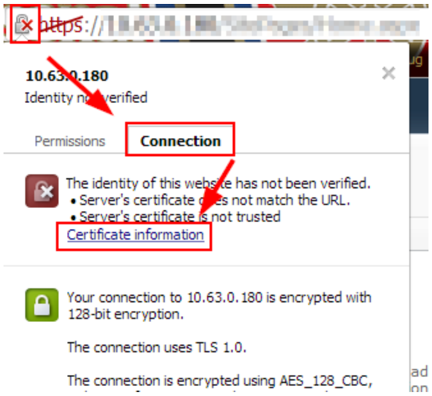
Rights Management Server can integrate with Microsoft SharePoint as a menu option available on your SharePoint sites. You can integrate Rights Management Server with both Microsoft SharePoint Online (for more information, refer to Integrating with SharePoint Online) or Microsoft SharePoint On-Premise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



https://[redacted]

10.63.0.180

Identity not verified

The identity of this website has not been verified.
- Server's certificate does not match the URL.
- Server's certificate is not trusted

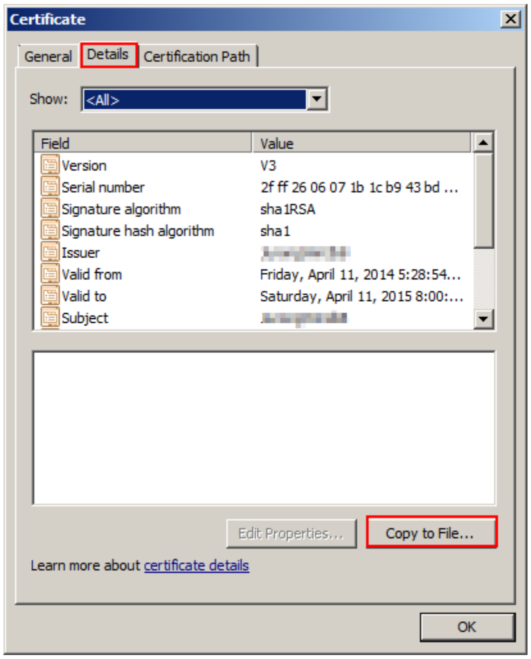
Certificate information

Your connection to 10.63.0.180 is encrypted with 128-bit encryption.

The connection uses TLS 1.0.

The connection is encrypted using AES_128_CBC,

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



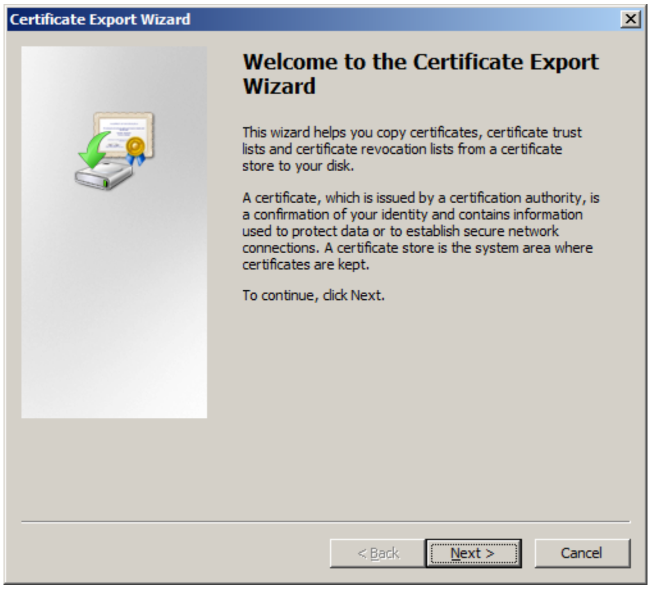
Certificate

Show: <All>

Field	Value
Version	V3
Serial number	2f ff 26 06 07 1b 1c b9 43 bd ...
Signature algorithm	sha1RSA
Signature hash algorithm	sha1
Issuer	[redacted]
Valid from	Friday, April 11, 2014 5:28:54...
Valid to	Saturday, April 11, 2015 8:00:...
Subject	[redacted]

Learn more about certificate details

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



Certificate Export Wizard

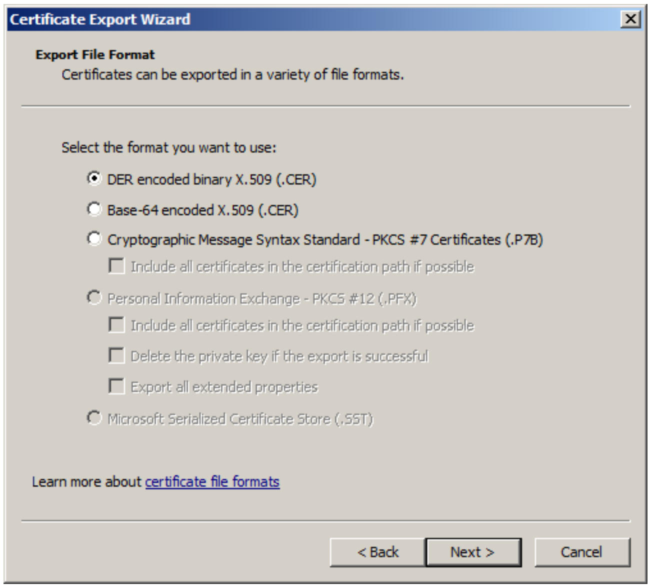
Welcome to the Certificate Export Wizard

This wizard helps you copy certificates, certificate trust lists and certificate revocation lists from a certificate store to your disk.

A certificate, which is issued by a certification authority, is a confirmation of your identity and contains information used to protect data or to establish secure network connections. A certificate store is the system area where certificates are kept.

To continue, click Next.

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



Certificate Export Wizard

Export File Format

Certificates can be exported in a variety of file formats.

Select the format you want to use:

● DER encoded binary X.509 (.CER)

○ Base-64 encoded X.509 (.CER)

○ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)

□ Include all certificates in the certification path if possible

○ Personal Information Exchange - PKCS #12 (.PFX)

□ Include all certificates in the certification path if possible

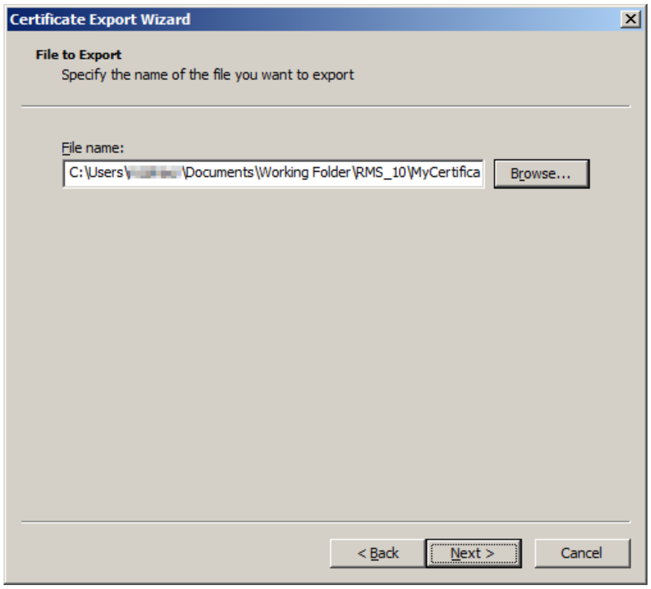
□ Delete the private key if the export is successful

□ Export all extended properties

○ Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

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



Certificate Export Wizard

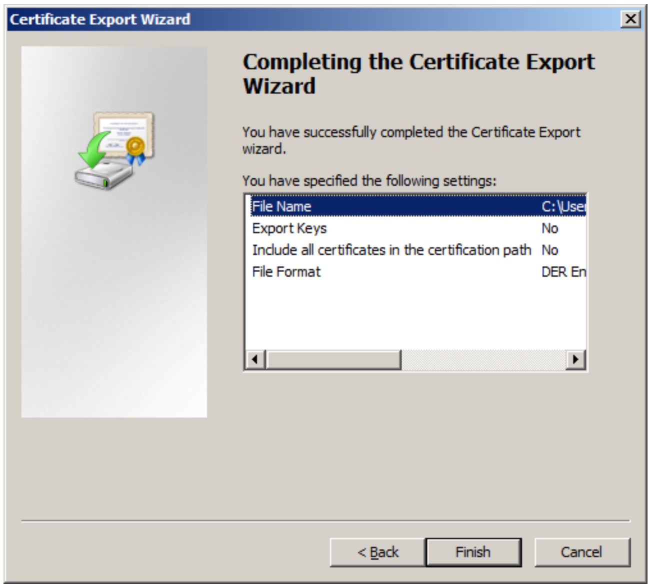
File to Export

Specify the name of the file you want to export

File name:

C:\Users\[redacted]\Documents\Working Folder\RMS_10\MyCertifica

6. Click **Finish**.



Certificate Export Wizard

Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

File Name	C:\Use
Export Keys	No
Include all certificates in the certification path	No
File Format	DER En

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.

NEXTLABS®

5 Integrating with SharePoint Online

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:

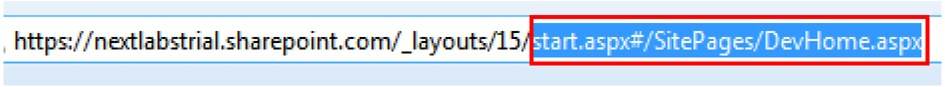
- Registering your SharePoint Online App
- Creating your SharePoint Online App
- Deploying your SharePoint Online App

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.

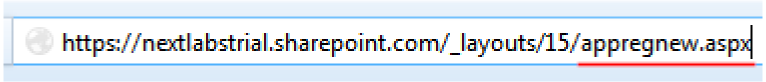
Note: The following steps are applicable if you want to register a High-Trust App for SharePoint Online as well.

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 `layout/15/` as indicated below:



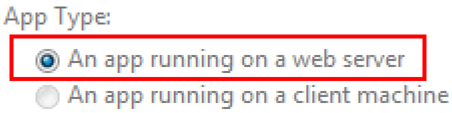
https://nextlabstrial.sharepoint.com/_layouts/15/start.aspx#/SitePages/DevHome.aspx

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.

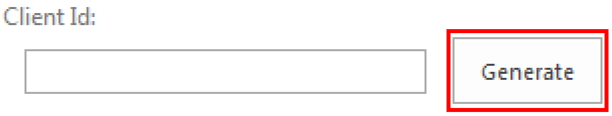


App Type:

● An app running on a web server

○ An app running on a client machine

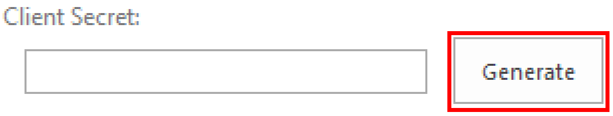
5. Click **Generate** to create a **Client Id** and note it down.



Client Id:

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:

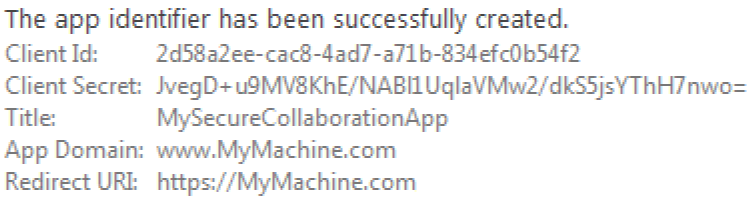
Note: The Client Secret value is used for your SharePoint Online App. This value expires after one year. Before you attempt to regenerate it, you must remove the **Client Id** and SharePoint Online App certificate name from your SharePoint deployment. Then you can update the **Client Id** value for your 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 Server, for example 10.168.23.28 or www.MyMachine.com** **NOTE:** 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 Server with the appropriate protocol included, for example https://10.168.23.28:8443 or https://MyMachine.com:8443 **NOTE:** 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/NABl1UqlaVMw2/dkS5jsYThH7nwo=

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 the ⚙ icon.

5. Click **Application Settings**.

6. Click **SharePoint App Settings**.

7. Click **Add SharePoint Application**.

8. Select the **SharePoint Type** as **SharePoint Online**.

9. Type the following details:

Field	Description
Display Name	This is the displayed name of the SharePoint App you want to configure.
App Client Id	This is the **Client Id** value that was generated during the SharePoint Online app registration. For more details, see Registering your SharePoint Online App.
App Client Secret	This is the Client Secret of the SharePoint App that you want to configure. **NOTE:** 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 **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.

10. Click **Save**.

11. Click the download icon for your SharePoint Online App ⬇.

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

12. 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"
```

6 Integrating with SharePoint On-Premise

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 serveres 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 Registering your SharePoint Online App.
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

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

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.xmll

```
<add key="AuthType" value="ADFS" />
<add key="IdentityClaimType" value="SMTP"/>
<add key="ClaimProviderType" value="SAML"/>
<add key="TrustedProviderName" value="your SAML Provider"/>
<add key="MembershipProviderName" value="your FbaMember"/>
```

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
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.**
IdentityClaimType	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.
ClaimProviderType	This is the claim provider type: FBA (Forms Based Access), SAML (Security Assertion Markup Language). The default value is SAML.
TrustedProviderName	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.
MembershipProivderName	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.

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

Configuring Protocol Binding for the Web App

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:

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**.

Creating your SharePoint On-Premise Apps

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 the ⚙ icon.
4. Click **Application Settings**.
5. Click **SharePoint App Settings**.
6. Click **Add SharePoint Application**.
7. Select the **SharePoint Type** as **SharePoint On-Premise**.
8. Type the following details:

Field	Description
Display Name	This is the displayed name of the SharePoint App you want to configure.

Remote App 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:
	`/Pages/Default.aspx`
	For example if your SharePoint Site App URL is:
	`https://myserver:4444`
	then you must type it as:
	`https://myserver:4444/Pages/Default.aspx`
	NOTE: If you have not changed the default port number (443) for your server then you don't need to specify the port number in the URL. Therefore, the above URL would be listed as:
	`https://myserver/Pages/Default.aspx`

App Client Id	This is the **Client Id** value that was generated during the SharePoint web app registration. For more details, see Registering your SharePoint Online App.

Field	Description
App Client Secret	This is the Client Secret of the SharePoint App that you want to configure.

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.

NEXTLABS®

7 Integrating with Dropbox

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
- Applying for Production Status

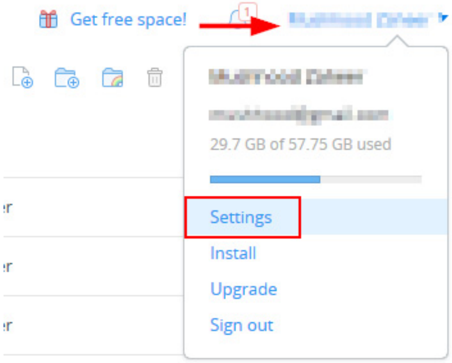
Configuring Rights Management Server for Dropbox Repositories

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

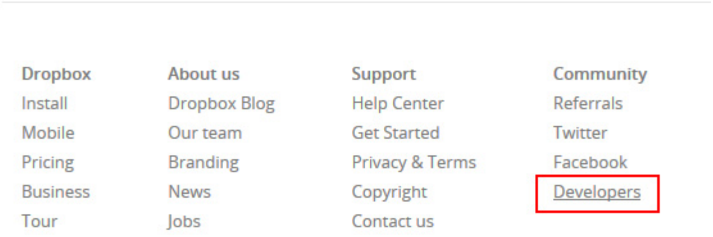
Note: The steps indicated below need to be done only once per Rights Management Server deployment. You must perform these configuration steps to be able to successfully add Dropbox repositories to your Rights Management Server.

Creating your Dropbox App for Rights Management Server

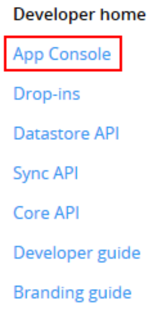
1. Login to the Dropbox website.
2. Click on your login name and then click **Settings**.



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



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



Developer home

App Console

Drop-ins

Datastore API

Sync API

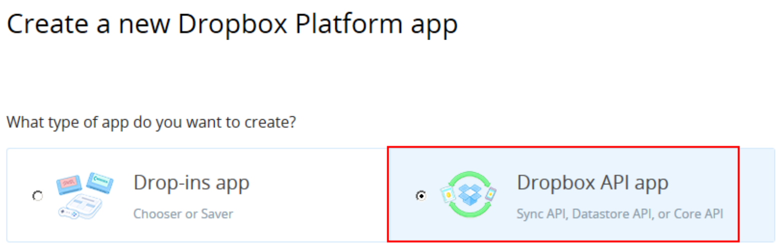
Core API

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**.



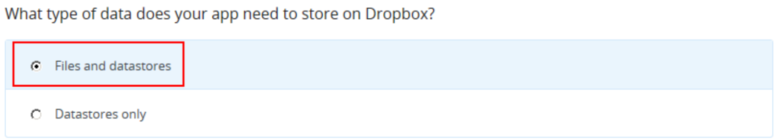
Create a new Dropbox Platform app

What type of app do you want to create?

○ Drop-ins app — Chooser or Saver

● Dropbox API app — Sync API, Datastore API, or Core API

7. Select **Files and datastores**.

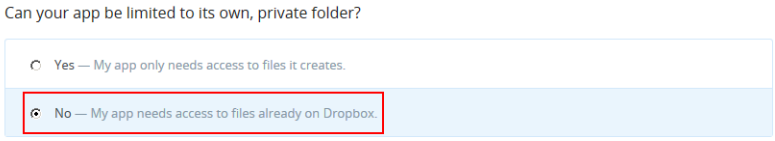


What type of data does your app need to store on Dropbox?

● Files and datastores

○ Datastores only

8. Select **No**.

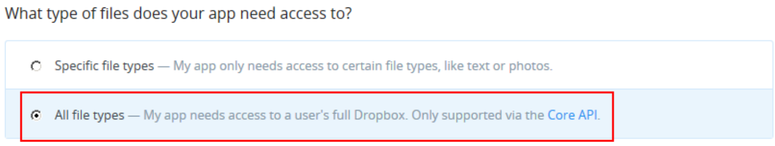


Can your app be limited to its own, private folder?

○ Yes — My app only needs access to files it creates.

● No — My app needs access to files already on Dropbox.

9. Select **All file types**.

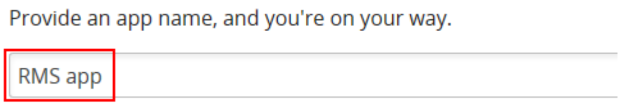


What type of files does your app need access to?

○ Specific file types — My app only needs access to certain file types, like text or photos.

● All file types — My app needs access to a user's full Dropbox. Only supported via the Core API.

10. Type your Dropbox app name.



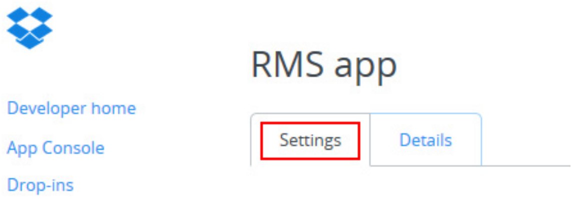
Provide an app name, and you're on your way.

RMS app

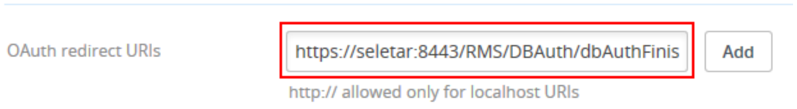
11. Click **Create app**.

Configuring your Dropbox App

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



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`

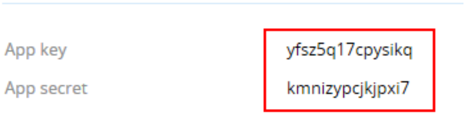


OAuth redirect URIs: https://seletar:8443/RMS/DBAuth/dbAuthFinis

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.

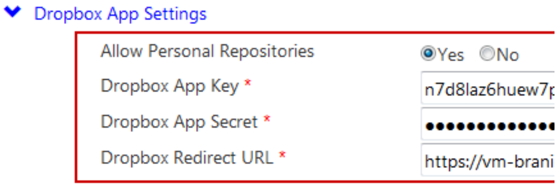


App key: yfsz5q17cpysikq

App secret: kmnizypcjkjpxi7

5. In the Rights Management Server web portal, click the ⚙ icon and navigate to **Application Settings > Dropbox App Settings**.

6. Copy the values for **App Key** and **App Settings** value to the **Dropbox App Key** and **Dropbox App Secret** fields respectively.



Dropbox App Settings

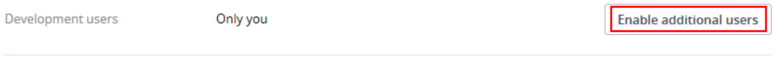
Allow Personal Repositories	● Yes ○ No
Dropbox App Key *	n7d8laz6huew7p
Dropbox App Secret *	●●●●●●●●●●●●●
Dropbox Redirect URL *	https://vm-brani

Note: Ensure that the **Dropbox Redirect URL** has the correct Rights Management Server value set. The format for the URL is:

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

7. 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.



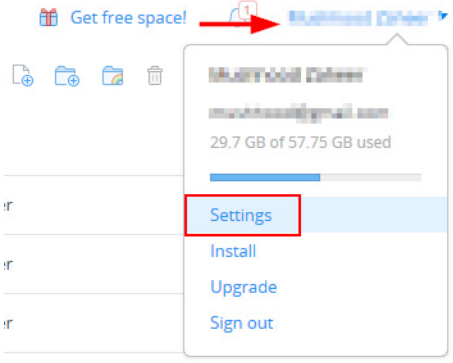
Development users Only you

Applying for Production Status

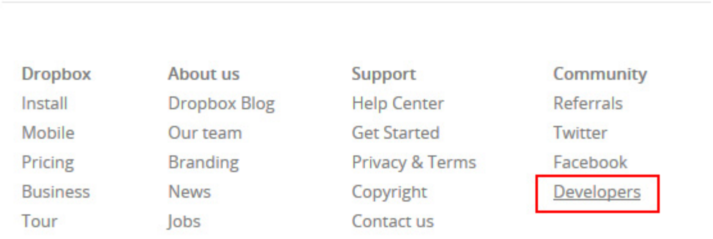
If you want your user base (assuming it is more than 100 users) to be able to link their Dropbox accounts as repositories then you must apply for the production status of your Dropbox app.

1. Login to the Dropbox website.

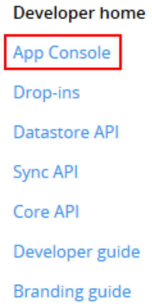
2. Click on your login name and then click **Settings**.



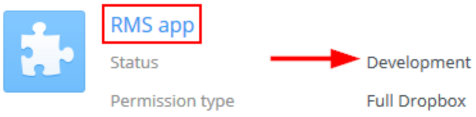
3. Scroll down to the bottom of the page and click the **Developers** link.



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



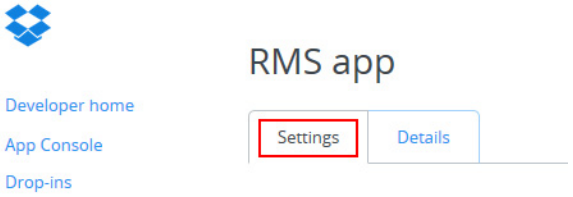
5. Click the Dropbox app you want to switch to Production status.



Status Development

Permission type Full Dropbox

6. Click the **Settings** tab.



7. Click **Apply for production**.

Status Development

Apply for production

8. Complete the Request production status form and click **Submit app**.

8 Access Control using Policies

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.

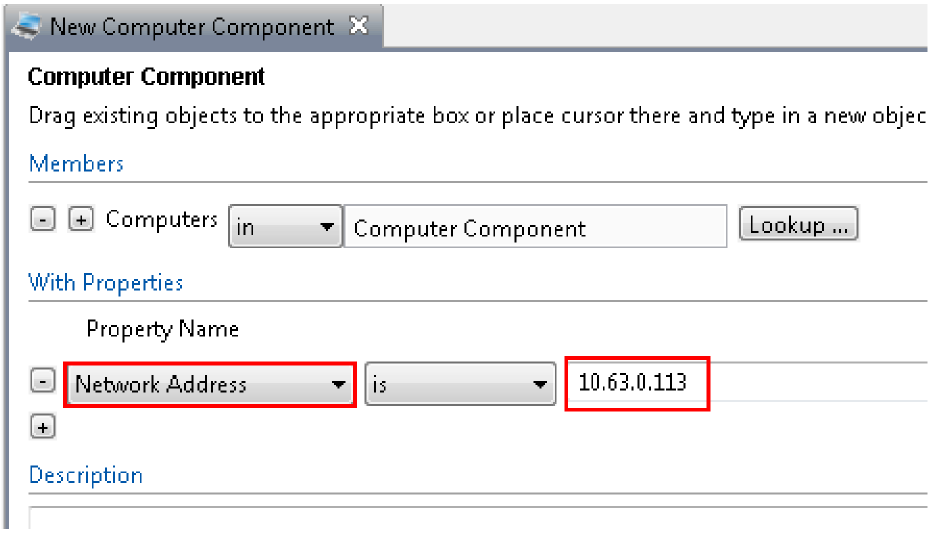
Enforcing IP Address Policies

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.



New Computer Component

Computer Component

Drag existing objects to the appropriate box or place cursor there and type in a new objec

Members

Computers in Computer Component

With Properties

Property Name

Network Address is 10.63.0.113

Description

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.

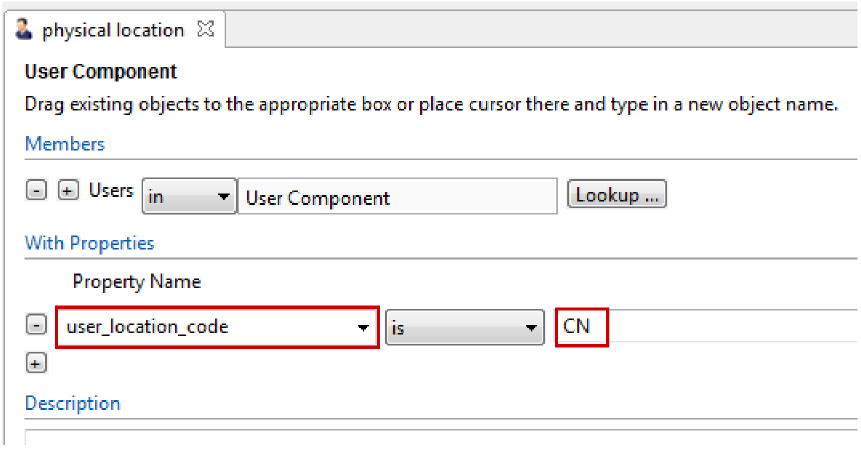
> *Note:* This feature is supported only for public IP addresses which adhere to the IPv4 standard.

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.



User Component

Drag existing objects to the appropriate box or place cursor there and type in a new object name.

Users in User Component

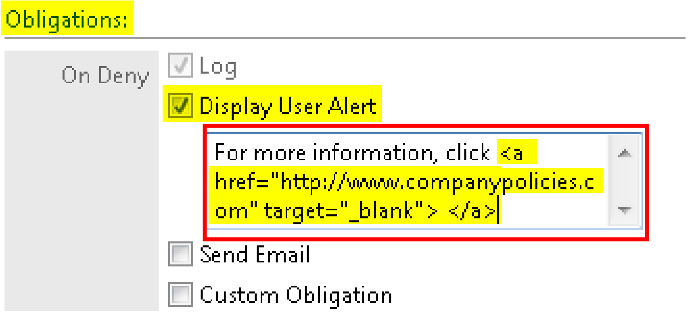
user_location_code is CN

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"> </a>

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

NEXTLABS®

9 Troubleshooting

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. **NOTE**: 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 Microsoft MSDN article.
Why do I see a Rights Management Server login screen when I select the **View in Rights Management Server** menu option in Microsoft SharePoint?	You can avoid being prompted for the Rights Management Server login screen each time you select the **View in Rights Management Server** in Microsoft SharePoint by adding both Microsoft SharePoint site and Rights Management Server 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.

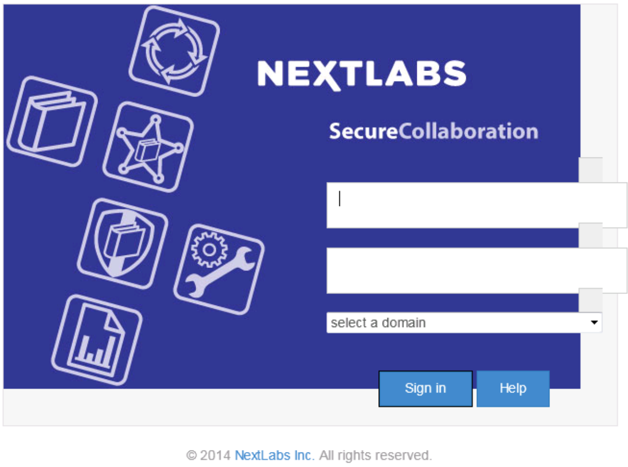
Question	Possible Answer
Why can’t I pinch zoom when viewing NXL protected documents in a mobile device?	The pinch zoom gesture is disabled for NXL protected files that are viewed on a mobile device. You can instead use the zoom in 🔍 and zoom out 🔍 icons present on your screen.

Why can’t I see my Microsoft SharePoint repository search results?	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:
	`$ssa = Get-SPEnterpriseSearchServiceApplication`
	`$ssa.MaxRowLimit = 10000`
	`$ssa.Update()`
	`iisreset`
	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.
	NOTE: 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.

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?	You might have configured the ICENet Server URL incorrectly during the installation. To update the ICENet Server URL, perform the following steps: 1.Open the following configuration file: <RMS_DATA_DIR>\javapc\config\commprofile.xml. 2.Edit the **DABSLocation** field with a proper ICENet Server URL. For example, https://my-icenet-server:8443/dabs. 3.Restart the Rights Management Server.
How do I decrypt bundle.bin in Embedded Java Policy Controller?	- Embedded Java PC currently doesn’t include the decrypt.bat utility that can be used to decrypt the policy bundle. - Copy the **decrypt.bat** and **decryptj** folders from any other Policy Controller installation to the <RMS_DATA_DIR>/javapc folder. - 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"
How do I change the port number used for Key Management after the RMS installation?	1. Stop RMS. 2. Specify the desired port number for the parameter **EMBEDDEDJPC_RMI_PORT_NUMBER** in the file **<RMS_DATA_DIR>/RMSConfig.properties**. 3.Specify the same port number for the parameter **rmi_registry_port** in the file **<RMS_DATA_DIR>/javapc/jservice/config/KeyManagementService.properties**. 4. Start RMS.

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

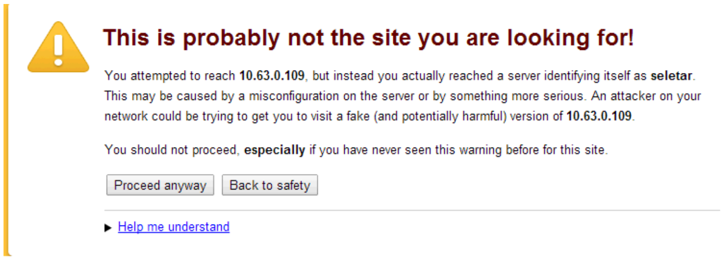
```
org.apache.axis2.AxisFault: javax.net.ssl.SSLException: Connection has
been shutdown: javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException:PKIX path building failed:
sun.security.provider.certpath.SunCertificate
```

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 is probably not the site you are looking for!

You attempted to reach **10.63.0.109**, but instead you actually reached a server identifying itself as **seletar**. This may be caused by a misconfiguration on the server or by something more serious. An attacker on your network could be trying to get you to visit a fake (and potentially harmful) version of **10.63.0.109**.

You should not proceed, **especially** if you have never seen this warning before for this site.

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.

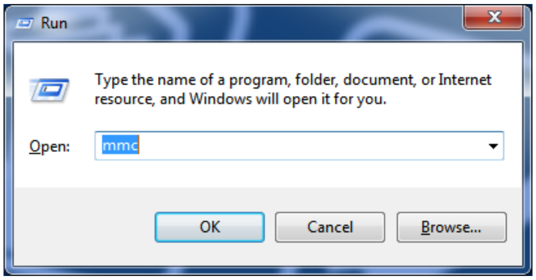
For more information, refer to Importing a Self Signed Certificate for the User.

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.

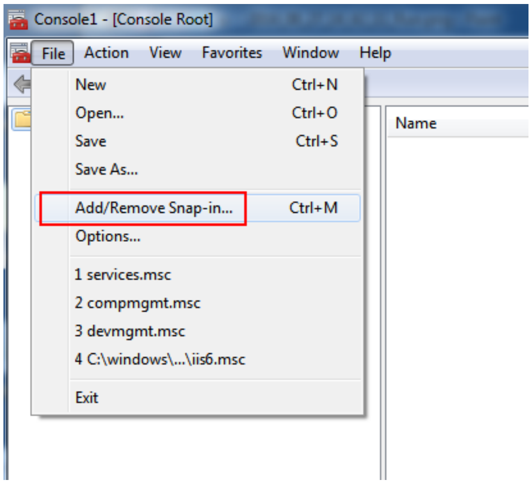
1. In your user's machine, navigate to **Start** > **Run** and type `mmc`.



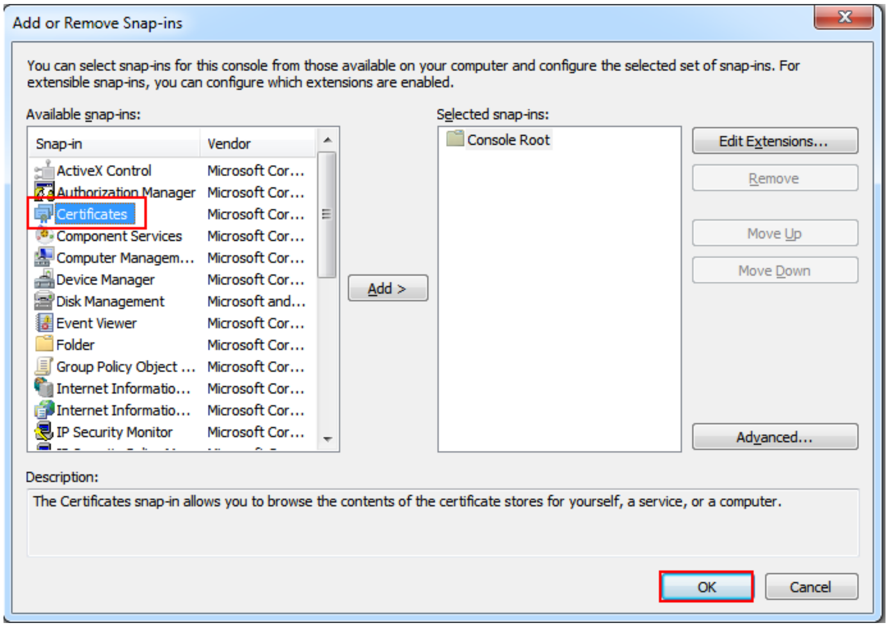
Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.

Open: 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**.


Add or Remove Snap-ins

You can select snap-ins for this console from those available on your computer and configure the selected set of snap-ins. For extensible snap-ins, you can configure which extensions are enabled.

Available snap-ins:

Snap-in	Vendor
ActiveX Control	Microsoft Cor...
Authorization Manager	Microsoft Cor...
Certificates	Microsoft Cor...
Component Services	Microsoft Cor...
Computer Managem...	Microsoft Cor...
Device Manager	Microsoft Cor...
Disk Management	Microsoft and...
Event Viewer	Microsoft Cor...
Folder	Microsoft Cor...
Group Policy Object ...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
Internet Informatio...	Microsoft Cor...
IP Security Monitor	Microsoft Cor...

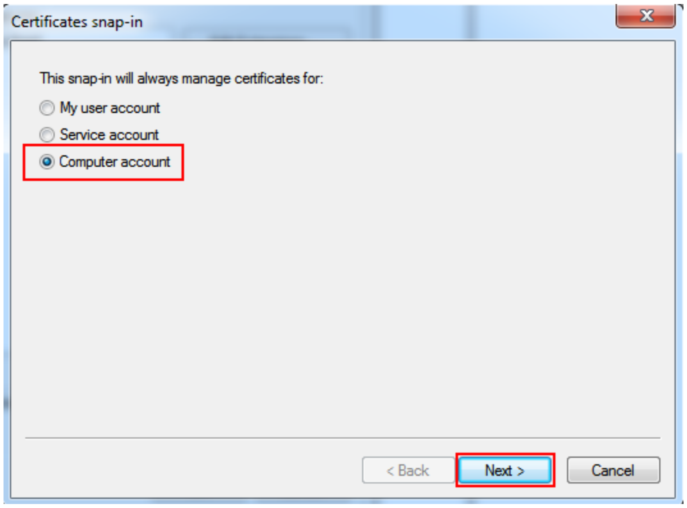
Selected snap-ins:

Console Root

Description:

The Certificates snap-in allows you to browse the contents of the certificate stores for yourself, a service, or a computer.

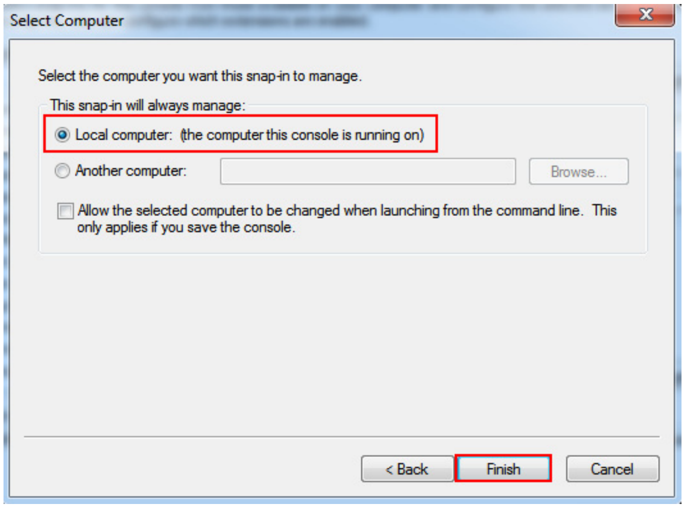
4. In the Certificate snap-in window, type select **Computer account** and click **Next.**


Certificates snap-in

This snap-in will always manage certificates for:

○ My user account
○ Service account
● Computer account

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


Select Computer

Select the computer you want this snap-in to manage.

This snap-in will always manage:

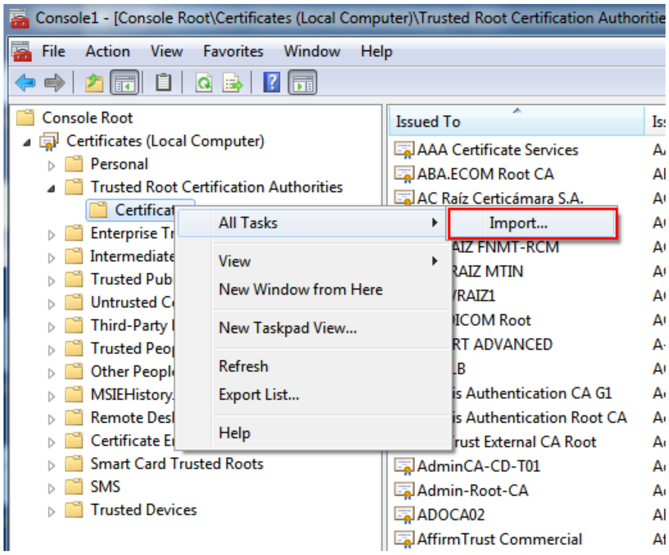
● Local computer: (the computer this console is running on)

○ Another computer:

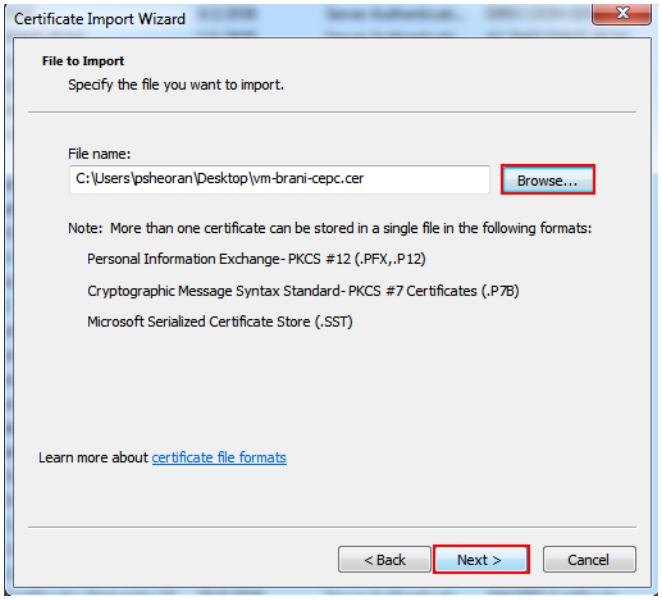
□ Allow the selected computer to be changed when launching from the command line. This only applies if you save the console.

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**.



Certificate Import Wizard

File to Import

Specify the file you want to import.

File name:

C:\Users\psheoran\Desktop\vm-brani-cepc.cer

Note: More than one certificate can be stored in a single file in the following formats:

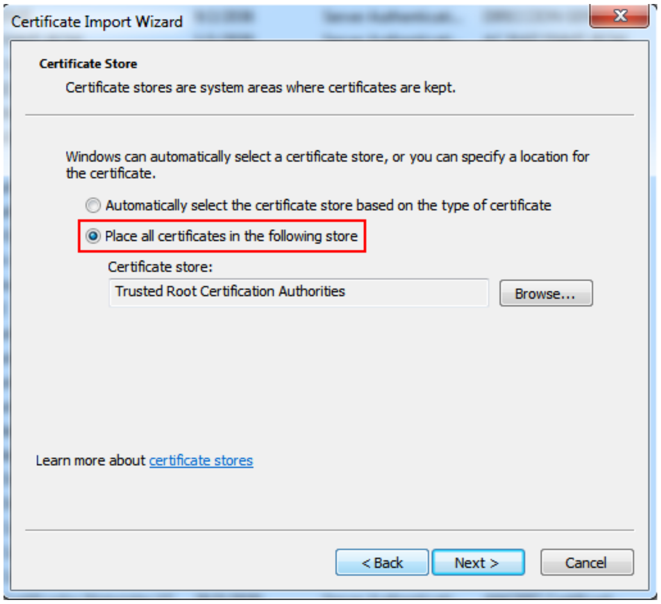
Personal Information Exchange- PKCS #12 (.PFX,.P12)

Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)

Microsoft Serialized Certificate Store (.SST)

Learn more about certificate file formats

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



Certificate Import Wizard

Certificate Store

Certificate stores are system areas where certificates are kept.

Windows can automatically select a certificate store, or you can specify a location for the certificate.

○ Automatically select the certificate store based on the type of certificate

● Place all certificates in the following store

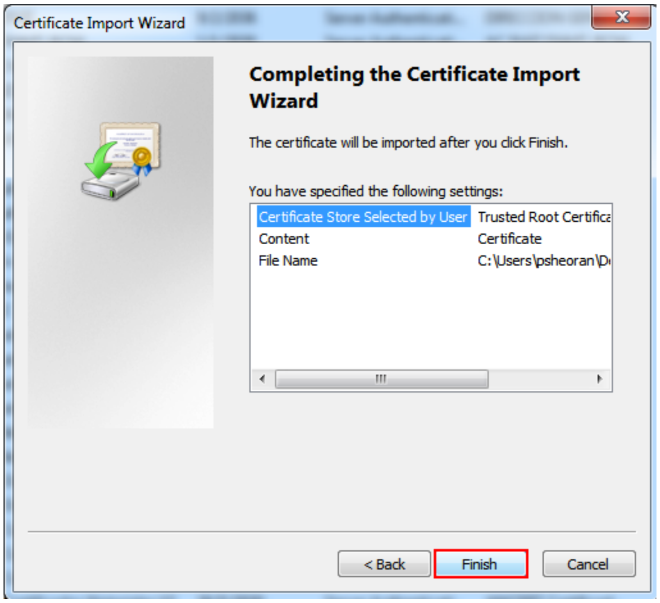
Certificate store:

Trusted Root Certification Authorities

Learn more about certificate stores

10. Click **Next.**

11. Click **Finish.**



Certificate Import Wizard

Completing the Certificate Import Wizard

The certificate will be imported after you click Finish.

You have specified the following settings:

Certificate Store Selected by User	Trusted Root Certifica
Content	Certificate
File Name	C:\Users\psheoran\D