1. Introduction ............................................. 7
   Welcome ............................................. 7
   Introducing Rights Management ......................... 8
      What is Persistent Protection? ....................... 8
      What are Access and Usage Rights? .................. 9
      What Are Document Securities? ...................... 9
      How Do Files Become Rights Managed? ............... 9
   Rights Management Client and the Information Life Cycle ....... 10
      Creation of Data .................................. 11
      Applying Protection ................................ 12
      Distribution ..................................... 12
      Access and Usage .................................. 12
   What Rights Can Be Enforced? .......................... 13
   Configuring the Rights ................................ 16

2. Setting Up Rights Management ............................... 19
   Setting Up Rights Management Client .................... 19
   Setting up your NextLabs Rights Management Server ...... 20
   Configuring your classification file ..................... 21
      Using the classification file ....................... 21
         Specifying the User Profiles ....................... 24
         Create the Labels ................................ 25
         List the Values ................................... 26
         Create a Trusted application ...................... 26
         Restrict the file formats that can be protected .... 27
   Using Policies to List Classification Labels ............... 27
      Specify the User Classification Custom Obligation ...... 27
      Sample Document Policy to Enable User Initiated Protection ...... 28
Deploying the classification file ................................................. 30
Key Management ................................................................. 31
  Creating a Shared Key Ring and a Shared Key ......................... 31
Where to Install Rights Management Components .......................... 32
  Key Management Server .................................................... 32
  Rights Management Client ............................................... 32
  Rights Management Server .............................................. 33
Before you Install ............................................................... 34
  Network Requirements .................................................... 34
  Supported Platforms ..................................................... 34
  Supported CAD Applications ........................................... 34
Creating your RMC Installation Package ..................................... 35
Installing Rights Management Client Manually .............................. 39
Setting up Rights Management Client ...................................... 42
Configuring the Rights Management Policy Model ......................... 43
  Configuring Rights Management Obligations .......................... 43
  Configuring Rights Management Resource Attributes ................. 43
  Configuring Special Actions ............................................ 44
3. Designing Access and Usage Policies ....................................... 47
Designing Access and Usage Policies ........................................ 47
Document Security Policies .................................................... 48
  Configuring Security Overlays ........................................... 48
  What Actions Can Be Enforced Upon? .................................. 50
Example Policy: View Security Overlay .................................... 50
  Create the New Policy and Define the Effect ......................... 50
  Define the Policy Subject .................................................. 50
  Define the Policy Action ................................................... 51
  Define the Policy Resource .............................................. 51
  Define the Obligations, Submit and Deploy the Policy ............... 51
Enabling Users to Protect Files .............................................. 53
4. Applying Protection .......................................................... 55
How Do Protected Files Behave? ............................................ 55
Removing Protection or Reclassifying ...................................... 55
5. Administration ....................................................................... 57
Introduction ............................................................................ 57
Key Management ..................................................................... 58
  Managing Keys ................................................................... 58
Server Key Management ........................................................ 59
  Using the Server Key Management Tool ................................. 59
Using the Server Key Management Tool ........................................ 60
More About Performing Key Rotations from the Server ................ 61
More About Backing up a Key Store ............................................. 61
Key Management Passwords ...................................................... 61
Monitoring Rights Management Clients ....................................... 63
Collecting Logs ......................................................................... 65
Enabling Debug Logs .................................................................. 65
Collecting Debug Logs ............................................................... 65
Viewing Activity Logs ............................................................... 66
Upgrading from RMC 8.0 or later .................................................. 67

6. Rights Management for JT2Go ................................................ 69
   About Rights Management for JT2Go ....................................... 70
   Before you Install .................................................................... 71
      Supported Platforms ........................................................... 71
   Installing Rights Management Client for JT2Go ....................... 72
Introduction

Welcome

Welcome to the product documentation for Rights Management Client (RMC). The following pages detail the installation, configuration, deployment as well as use of RMC.

Protecting proprietary information is critical to all businesses. However the modern day business operation involves collaboration with vendors that are not included in the company’s IT network. Therefore guaranteeing information security or preventing the risk of intellectual property falling into the wrong hands is challenging.

One of the methods of extending control outside of your IT network is to adopt file encryption as the primary tool to protect against any information security risks associated with handling proprietary information.

Rights Management Client allows the handlers of important information to quickly classify and encrypt content before handing it over to anybody. The information recipient can only view this information with RMC and an authorized user account.
Introducing Rights Management

Rights Management (sometimes “Digital Rights Management” or “Enterprise Rights Management”), refers to the family of document-level controls that ensure protected data is accessed and used properly within a Policy Domain, and not accessible outside of it. A “Policy Domain” is a logical construct that includes all hosts where Rights Management is installed—in other words, where access and usage policies can be enforced. The Policy Domain (the shaded area in the figure below) may or may not correspond to a physical IT Domain (represented by the dashed line). For instance, the Policy Domain may extend to mobile and remote users who can log in and off the network and who have Rights Management Client installed on their laptops, while not including computers within the IT Domain where enforcers are not installed.

To reinforce the Policy Domain and maintain rights within it, Rights Management combines three kinds of application controls:

- Persistent Protection (classification and encryption)
- Document-Level Access and Usage Rights
- Document Securities

Each is discussed in more detail below.

What is Persistent Protection?

Persistent Protection refers to two aspects that are central to Rights Management: Encryption and file classification.

Encryption reinforces a Policy Domain by preventing unauthorized users (those not in the domain) from accessing protected data. Encryption provides a layer
of protection that lies on top of granular Access and Usage and Document Security policies. This protection is “persistent,” as it stays with the document wherever it goes, no matter how or where the file is accessed or used (inside or outside the Policy Domain).

Protection is also persistent due to file classification (that is, the injection of tags into file headers that can be referenced by policies). When in encrypted format, classification values persist as the document is accessed anywhere.

Once encryption and classification are applied, they are transparent to end users, files, and applications. This means authorized users can access protected content seamlessly without interrupting their work, and that encryption and classification is independent of file type and application.

Encryption keys can be managed and administered centrally, with the NextLabs Policy Server automatically exporting key rotations and other updates to endpoints in the Policy Domain. For more information about administering encryption keys, see Key Management.

What are Access and Usage Rights?

NextLabs Rights Management also enables policy designers to apply granular, document-level controls that govern how users work with rights managed content. Access and Usage controls can take into consideration the identity attributes of users, the classification tags of the files being accessed and used, and the context of use (location, time of day). In addition, as is discussed in more detail in What Rights Can Be Enforced?, policies can target very specific user actions, from opening a document, to copying content to a clipboard, to taking screen captures, and more.

What Are Document Securities?

A subset of Access and Usage policies (which target documents-in-use in their digital format), are Document Security policies (which change the appearance of documents as they migrate across different media). You can apply Security Overlays to documents viewed in digital format, while not changing document content (as watermarks do). Document Securities are thus like the last line of defense—to “stamp” or otherwise alter how content displays, to educate users and govern how content is used as it possibly leaves the control of the digital Policy Domain. Example Document Security policies are presented in Document Security Policies.

How Do Files Become Rights Managed?

Rights protection can be applied to documents in two ways:

- Manually by a User with the NextLabs Rights Management Client installed on their machine
- Automatically by a NextLabs Document Control Server

Note: For more information about the various ways to mark files for encryption, see Applying Protection.
Rights Management Client and the Information Life Cycle

Rights Management Client is a required component for an implementation of Rights Management where the user needs to edit the encrypted document being viewed.

If a business requirement includes the need to protect files while they reside within a file server or Enterprise Collaborative Application (like SAP or SharePoint), the implementation will also require NextLabs Document Control Server. In this case, it will be necessary to coordinate how protection is applied at the server and endpoint.

The following figure demonstrates the functions of RMC as information moves through stages of the information life cycle: Creation, Protection, Distribution, and Access and Usage. Each stage is addressed in more detail in subsequent sections.
Introduction

**Creation of Data**

The point of origination (where data initially becomes rights managed) is the distinguishing factor between Document Control Server and Rights Management Client. Rights Management Client and Document Control Server are triggered by different user “events,” which lead to encryption and classification of data. For Document Control Server, the point of origination is data being uploaded to a file server or enterprise applications (like SAP or SharePoint). For Rights Management Client, the point of origination is the event of data being created, edited, and/or copied or moved on an endpoint.

---

**Figure 1-2: Rights Management Client**

1. **Creation, Protection & Sharing**
   - File is created, modified, tagged, and then converted into an NXL protected document shared from an endpoint.

2. **Distribution**
   - Upload the file to a server or share it over email.

3. **Access and Usage**
   - Policies control how protected files are handled at an endpoint.
     - Print?
     - Edit?
     - Copy?
     - Classify?
     - Display Overlay?
     - Decrypt?
Applying Protection

Rights Management Client enables the user to protect and classify documents at their own discretion. The user can select the types of classification labels to associate with the document including a set of sub-labels (multiple level support) to convert the document into a NXL protected document.

The NXL Protected document can only be viewed by users that have the appropriate View rights based on the policies you have deployed to the Rights Management Client.

Distribution

NXL protected documents can be distributed across a policy domain and accessed as well as used by authorized users.

Access and Usage

For protected files, policies can govern how authorized users handle them at the endpoint, for instance, whether and by whom they can be edited, printed, saved, and so on. In addition, Document Security policies, a subset of Access and Usage policies, can govern the appearance of files when they are displayed on a screen.

For example for view overlay policies, see Document Security Policies.
What Rights Can Be Enforced?

Access and Usage policies can be designed to evaluate the following rights for document handling actions as indicated in the table below.

Currently all rights for the Open action are evaluated and enforced via policy evaluations.

*Note:* These actions must be manually added to your Policy Server configuration file before they will display as Actions in Policy Studio. These actions must be configured in the `<ActionList>` node of the Policy Server’s `configuration.xml` file.

<table>
<thead>
<tr>
<th>Right</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>Open a file for viewing</td>
</tr>
</tbody>
</table>
| Edit     | Change the contents of an existing NXL protected document or item. Specifically this means to edit the content of an existing document using the File > Save menu option.  
*Note:* Classification and encryption are retained after the document is edited. |
| Print    | Print any file, either to a printer device for hard copy, or an output file of any format.  
*Note:* If the document is printed to a soft copy, then the rights protection is not automatically applied to the new soft copy. |
| Clipboard| Copy or cut a portion of the file’s contents and paste it to any location (either in the same file or another file).  
This action is enforced when a user selects the content and tries to copy it. That is, although the real point is to prevent pasting to unsecured locations, the user is prevented from copying it to the clipboard. |
| SaveAs   | Make a duplicate of a file to the same file type. Specific actions include:  
Within an application, select File > Save As and create a copy of the file to the same file format.  
*Note:* If a file is saved to another format, the encryption and classification labels are inherited. |
| Decrypt  | Remove protection from a NextLabs protected document                       |
| ScreenCap| Copy part or all of computer screen as an image file using the Print Scrn key and Windows clipboard, specialized screen capture applications, or screen capture features inside general graphics applications.  
*Note:* Only the protected content is blocked. |
NextLabs Rights Management Client supports rights across three different application categories:

- Microsoft Office and Adobe Reader
- CAD applications
- Generic applications

The following table lists the rights that are supported for each application category:

<table>
<thead>
<tr>
<th>Rights</th>
<th>Behavior (No Rights Granted)</th>
<th>Behavior (Rights granted)</th>
<th>Microsoft Office</th>
<th>CAD application</th>
<th>Generic application</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>The document is not opened by the application.</td>
<td>The document is opened by the application.</td>
<td>Yes (with overlay obligation)</td>
<td>Yes (without overlay obligation)</td>
<td>Yes (without overlay obligation)</td>
</tr>
</tbody>
</table>
| Edit   | Save option is blocked when the user tries to save via:  
- File > Save menu.  
- Any keyboard shortcut that can be used to trigger a save action (Ctrl + S). | No obligations supported. Saved documents are still rights protected with their original classification. | Yes | Yes | Yes |
| Print  | Print option is blocked when the user tries to print via:  
- File > Print menu.  
- Keyboard shortcut that could be used to trigger a print job (Ctrl + P)  
- Shortcut menu in the user interface  
- Explorer context menu > Print | No obligations supported. Printed document (hard copy or soft copy) is not rights protected. | Yes | No | No |

NOTE: If the send right is granted, then the document is not protected when it is sent to another user or location.

NOTE: This right does not control File > Save As because this right does not represent a change to the original document.

Send
Send should be used to target the behavior of sending a file outside the local machine. The Send action does not target a specific destination (send to any location outside local machine).

The Send action might apply to different menu items in different applications. For example, from within Acrobat Reader, this could be “Create PDF Online,” “Send for Shared Review,” or “Collaborate.” You can also select “Send” from the file menu in many Microsoft Office applications.
<table>
<thead>
<tr>
<th>Rights</th>
<th>Behavior (No Rights Granted)</th>
<th>Behavior (Rights granted)</th>
<th>Microsoft Office ---- Adobe Reader</th>
<th>CAD application</th>
<th>Generic application</th>
</tr>
</thead>
</table>
| Clipboard| The copy action for document content to system or application’s clipboard function is blocked when a user tries to copy-paste via:  
- Edit > Copy menu, and Edit > Cut menu.  
- Copy and Cut from any shortcut menu.  
- Any keyboard shortcut that can be used to trigger a copy-paste (for example, Ctrl+C or Ctrl+X). | No obligations supported. Copied content is not encrypted and the destination file does not automatically inherit rights protection. | Yes                             | No               | No                   |
| SaveAs   | Save As option is blocked when you attempt to save a copy of the protected document via:  
- File > Save As menu.  
- File > Export menu.  
- Any keyboard shortcut that can be used to trigger a copy. | No obligations supported. Save as action is allowed, and the resulting new copy of the document is automatically protected with the same classification labels as the source document.  
**NOTE:** Classification and encryption is inherited regardless of the file format of the new copy. | Yes                             | Yes                           | No                   |
| Decrypt  | The user cannot convert a NXL protected document back to its native file format:  
Any UI that can be used to decrypt (remove protection) from a protected document is disabled. | No obligations supported. The user is able to convert a NXL protected document back to its original native file format. The NXL protection is removed after this operation. | Yes                             | Yes                           | Yes                  |
| ScreenCap| If the user attempts to use the screen capture option then any area of the captured image that contains protected content is blacked out. The screen capture is blocked for the user if attempted via:  
- any keyboard shortcut that can be used to trigger a system print screen  
- any screen capture tools from doing a grab screen  
**NOTE:** Screen capture functions from Windows native feature or 3rd party screen capture tools are NOT blocked. | No obligations supported. Users are able to perform a screen capture and the captured image is not altered. | Yes                             | No               | No                   |
| Send     | Attempts to Share or email other user are blocked when the user tries to send via:  
- File > Share/Send/Email menu.  
- Any keyboard shortcut that could be used to trigger a send  
- Shortcut menu items that can be used to trigger a send | No obligations supported. The user can attach the unprotected file to another user or location. | Yes                             | No               | No                   |
Introduction

---

### Rights Management Client 9.0 • Rights Management

#### Configuring the Rights

Before you can create a policy which uses the rights mentioned above, you must ensure that your NextLabs Control Center’s `configuration.xml` file contains the following xml code in the `<ActionList>` section:

<table>
<thead>
<tr>
<th>Right</th>
<th>xml code</th>
</tr>
</thead>
<tbody>
<tr>
<td>View</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_VIEW&lt;/Name&gt; &lt;DisplayName&gt;View Right&lt;/DisplayName&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;ShortName&gt;R0&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt;</td>
</tr>
<tr>
<td>Edit</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_EDIT&lt;/Name&gt; &lt;DisplayName&gt;Edit Right&lt;/DisplayName&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;ShortName&gt;R1&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt;</td>
</tr>
<tr>
<td>Print</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_PRINT&lt;/Name&gt; &lt;DisplayName&gt;Print Right&lt;/DisplayName&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;ShortName&gt;R2&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt;</td>
</tr>
<tr>
<td>Clipboard</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_CLIPBOARD&lt;/Name&gt; &lt;DisplayName&gt;Copy to Clipboard Right&lt;/DisplayName&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;ShortName&gt;R3&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt;</td>
</tr>
<tr>
<td>SaveAs</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_SAVEAS&lt;/Name&gt; &lt;DisplayName&gt;Save As Right&lt;/DisplayName&gt;</td>
</tr>
<tr>
<td></td>
<td>&lt;ShortName&gt;R4&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt;</td>
</tr>
</tbody>
</table>

#### Rights Behavior

<table>
<thead>
<tr>
<th>Rights (No Rights Granted)</th>
<th>Rights (Rights granted)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Classify</td>
<td>No obligations supported. The user is able to read and modify all classification labels for the document. Any user interface that can be used to classify protected document is disabled</td>
</tr>
<tr>
<td>Microsoft Office CAD</td>
<td>Yes</td>
</tr>
<tr>
<td>Adobe Reader</td>
<td>Yes</td>
</tr>
<tr>
<td>Generic application</td>
<td>Yes</td>
</tr>
</tbody>
</table>

---

6/3/16
For more information about configuring Custom Actions for your NextLabs Control Center, refer to **Configuring Special Actions**.

<table>
<thead>
<tr>
<th>Right</th>
<th>xml code</th>
</tr>
</thead>
<tbody>
<tr>
<td>Decrypt</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_DECRYPT&lt;/Name&gt; &lt;DisplayName&gt;Remove Protection Right&lt;/DisplayName&gt; &lt;ShortName&gt;R6&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt; &lt;/Action&gt;</td>
</tr>
<tr>
<td>ScreenCap</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_SCREENCAP&lt;/Name&gt; &lt;DisplayName&gt;Screen Capture Right&lt;/DisplayName&gt; &lt;ShortName&gt;R7&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt; &lt;/Action&gt;</td>
</tr>
<tr>
<td>Send</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_SEND&lt;/Name&gt; &lt;DisplayName&gt;Send Right&lt;/DisplayName&gt; &lt;ShortName&gt;R8&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt; &lt;/Action&gt;</td>
</tr>
<tr>
<td>Classify</td>
<td>&lt;Action&gt; &lt;Name&gt;RIGHT_CLASSIFY&lt;/Name&gt; &lt;DisplayName&gt;Classify Right&lt;/DisplayName&gt; &lt;ShortName&gt;R9&lt;/ShortName&gt; &lt;Category&gt;Rights&lt;/Category&gt; &lt;/Action&gt;</td>
</tr>
</tbody>
</table>
Rights Management works through the interaction of several NextLabs components. These instructions assume you have already installed and configured some of these components, including the NextLabs Control Center.

The recommended order of setting up your Rights Management Client deployment is to first ensure your NextLabs Control Center is configured properly.

This chapter covers the following sections:

- Setting up your NextLabs Rights Management Server
- Configuring your classification file
- Deploying the classification file
- Key Management
- Where to Install Rights Management Components
- Before you Install
- Installing Rights Management Client Manually
- Setting up Rights Management Client
- Configuring the Rights Management Policy Model
NextLabs Rights Management Client (RMC) is a policy enforcement agent that is deployed on the end user’s computer in your company’s IT network. The policies that are deployed on RMC are created in NextLabs Policy Studio. The Policy Author creates the company policies in the NextLabs Control Center database and also initiates the command to submit and deploy them to all computers on your network.

You must have the NextLabs Control Center and the NextLabs Rights Management Server deployed as well as configured. Your policies must be created (via the NextLabs Policy Studio) and ready to deploy - before you install Rights Management Client.

Prior to deploying Rights Management Client (RMC) you must perform the following steps on your NextLabs Rights Management Server:

- Configuring your classification file
- Deploying the classification file
- Key Management
Configuring your classification file

Rights Management Client (RMC) enables a user to protect and classify documents. Your RMC deployment can be configured to allow all users to classify documents using a default set of classification labels, which you can specify in the RMC_Classification.xml file.

If you do not have RMC_Classification.xml file then you can contact NextLabs support to receive a copy.

You can also configure your RMC deployment to list different sets of classification labels based on the user. For more information refer to, Using Policies to List Classification Labels.

Using the classification file

In the RMC_Classification.xml file, you can configure the hierarchy of classification labels that your users must select whenever they classify a document. The different labels that you specify in the RMC_Classification.xml file are displayed in the user interface of the Rights Management Client.

You can implement a classification hierarchy that has multiple sub-labels (refer to Figure 2-1).

In the example listed below, the user is presented with initially two label options (Sensitivity and Program). After a Program value is selected, a third label is displayed (Jurisdiction).
Depending on which value is chosen for the Jurisdiction label, the user can select different types of classification labels (TAA, EAR, or BAFA) and set appropriate values.

![Figure 2-1: A typical classification hierarchy](image_url)
The classification tags are specified in the **RMC_Classification.xml** file. The corresponding xml content for the above classification hierarchy is indicated below.

```xml
<Classify>
  <Profiles>
    <Default 0.1/Default>
      <Engineer 0.1/Engineer>
        <Product 0/Product>
      </Engineer>
    </Default>
  </Profiles>
  <Labels>
    <Label id="0" name="Sensitivity" display-name="Sensitivity" mandatory="true"
      multi-select="false" default-value="0">
      <Value priority="0" value="Non Business"/>
      <Value priority="1" value="General Business"/>
      <Value priority="2" value="Proprietary"/>
      <Value priority="3" value="Confidential"/>
    </Label>
    <Label id="1" name="Program" display-name="Program" mandatory="true"
      multi-select="false" default-value="0">
      <Value value="FR-01" sub-label="0"/>
      <Value value="FR-02" sub-label="2"/>
      <Value value="FR-03" sub-label="3"/>
    </Label>
    <Label id="2" name="Jurisdiction" display-name="Jurisdiction" mandatory="true"
      multi-select="false" default-value="0">
      <Value value="ITAA" sub-label="0"/>
      <Value value="WAP" sub-label="4"/>
      <Value value="BAPA" sub-label="5"/>
    </Label>
    <Label id="3" name="ITAA" display-name="ITAA Property" mandatory="true"
      multi-select="true" default-value="0">
      <Value value="ITAA-01"/>
      <Value value="ITAA-02"/>
      <Value value="ITAA-03"/>
    </Label>
    <Label id="4" name="WAP" display-name="WAP Property" mandatory="true"
      multi-select="true" default-value="0">
      <Value value="WAP-01"/>
      <Value value="WAP-02"/>
      <Value value="WAP-03"/>
    </Label>
    <Label id="5" name="BAPA" display-name="BAPA Property" mandatory="true"
      multi-select="true" default-value="0">
      <Value value="BAPA-01"/>
      <Value value="BAPA-02"/>
      <Value value="BAPA-03"/>
    </Label>
  </Labels>
</Classify>
```

You must define the **Profiles** and **LabelList** sections, in the **RMC_Classification.xml** file.

The **Profiles** consists of nodes that represent different user groups that log in to the Rights Management Client. The numerical values specified for each user group indicates the id of each **Label** which is displayed for a user that belongs to a particular profile name (or user group).

The **LabelList** consists of each **Label** you want to display in the RMC classification user interface. Each **Label** consists of the respective **Value** nodes.

In the **RMC_Classification.xml** file you must:

- **Specifying the User Profiles**

---

Rights Management Client 9.0 • Rights Management
Setting Up Rights Management

- Create the Labels
- List the Values
- Create a Trusted application
- Restrict the file formats that can be protected

Specifying the User Profiles

Rights Management Client enables you to specify different classification tags in the user interface depending on which user is logged in.

You can configure this using document policies which trigger RMC to display classification tags. For more information, refer to Using Policies to List Classification Labels. These policies rely on the nodes listed in the Profiles node in your RMC_Classification.xml file.

In your RMC_Classification.xml file, in the Profiles node you must specify the different user profiles as nodes. Each node represents different logical group associations for a user.

The numerical values listed for each Profiles node indicates which Label is displayed for a user associated with a particular user profile.

Each numerical id must correspond to the id of a Label in your RMC_Classification.xml file. You must specify appropriate user profiles for your user base as indicated below:

```xml
<Classify>
  <Profiles>
    <Default>0,1</Default>
    <Engineer>0,1</Engineer>
    <Product>0,1</Product>
  </Profiles>
  <LabelList>
    <Label id="0" name="Sensitivity" display-name="" multi-select="false" default-value="0">
      <VALUE priority="0" value="Non Business"/>
      <VALUE priority="1" value="General Business"/>
      <VALUE priority="2" value="Proprietary"/>
      <VALUE priority="3" value="Confidential"/>
    </Label>
    <Label id="1" name="Program" display-name="" multi-select="false" default-value="0">
      <VALUE value="FR-Q1" sub-label="2"/>
      <VALUE value="FR-Q2" sub-label="2"/>
      <VALUE value="FR-Q3" sub-label="2"/>
    </Label>
  </LabelList>
</Classify>
```

Note: In order for a user to view classification labels there must be a policy deployed which triggers a classify obligation and states one of the user profiles from RMC_Classification.xml file in the Group field of the obligation. If you do not specify a value for the Group field then the Default user profile (indicated in the xml code above) is used to display the classification labels. For more information on writing a policy which specifies a custom obligation to classify, refer to Using Policies to List Classification Labels.
Create the Labels

In your RMCClassification.xml file, create the Label nodes as indicated in the image below.

```xml
<LabelList>
  <label id="0" name="Sensitivity" display-name="Sensitivity" mandatory="true"
    multi-select="false" default-value="0">
    <VALUE priority="0" value="Non Business" />
    <VALUE priority="1" value="General Business" />
    <VALUE priority="2" value="Proprietary" />
    <VALUE priority="3" value="Confidential" />
  </label>
</LabelList>
```

*Note:* Any classification labels longer than 50 characters are automatically truncated in the drop down list of the Rights Management Client classification window.

The following table details one of the Label nodes highlighted above:

<table>
<thead>
<tr>
<th>Label Attribute</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>id</td>
<td>This is the numerical id of your Label, which is used to identify it for your classification hierarchy. <strong>NOTE:</strong> This value must be unique.</td>
</tr>
<tr>
<td>name</td>
<td>This is the name of your Label.</td>
</tr>
<tr>
<td>display-name</td>
<td>This is the term that is displayed in the RMC user interface to represent your Label.</td>
</tr>
<tr>
<td>mandatory</td>
<td>This value indicates if the Label is a mandatory value or optional. A true value indicates that the Label is mandatory.</td>
</tr>
<tr>
<td>multi-select</td>
<td>This value indicates if the Label can have multiple values. A true value indicates that the Label is mandatory. <strong>NOTE:</strong> If this label attribute is set to true, only 7 multi values are supported.</td>
</tr>
<tr>
<td>default-value</td>
<td>This value indicates if this Label has a default value. A &quot;0&quot; value indicates no default value, and the label is displayed with a blank value. However, (referring to the sample xml code listed above) a value of &quot;1&quot; indicates the default value is &quot;Non Business&quot; and a value of &quot;2&quot; indicates the default value as &quot;General Business&quot;.</td>
</tr>
<tr>
<td>VALUE</td>
<td>This is the xml node which indicates a possible value of the Label. For more information refer to List the Values.</td>
</tr>
<tr>
<td>priority</td>
<td>This is the attribute that specifies the priority of the label value which the user selects. For example, if the user selects a label value with a priority value of &quot;3&quot; (&quot;Confidential&quot;), then the user cannot reclassify (assuming the user has classify rights) the label to a value lower than &quot;3&quot;. Therefore according to the xml code listed above, the user cannot reclassify the Sensitivity label value to anything other than &quot;Confidential&quot;.</td>
</tr>
</tbody>
</table>
List the Values

In the RMC_Classification.xml file, you must specify the possible Value nodes for each Label. You can define each VALUE as indicated in the image below:

```xml
  <Label id='1' name='Program' display-name='Program' mandatory='true'
      multi-select='false' default-value='0'>
    <VALUE value='PR-01' sub-label='1'/>
    <VALUE value='PR-02' sub-label='2'/>
    <VALUE value='PR-03' sub-label='3'/>
  </Label>
```

The following table details one of the VALUE nodes highlighted above:

<table>
<thead>
<tr>
<th>VALUE Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>value</td>
<td>This attribute value indicates the actual value that is displayed for a Label. NOTE: This attribute supports a value which is up to 50 characters long.</td>
</tr>
<tr>
<td>sub-label</td>
<td>This is the numerical id of the Label you want displayed (as the sub-label) if this value is selected.</td>
</tr>
</tbody>
</table>

Create a Trusted application

In order to view an NXL file in plain text, the application must be trusted and the user must be granted proper access rights. If the application is not trusted, the NXL file will be in an encrypted format. To trust the application, you can set the name of the application in the Policy Studio Application component or you can add it to the RMC_Classification.xml file under the section WhiteList as shown in the example below. After the application is trusted, you can grant suitable access rights to view an NXL file using the Policy Studio.

```xml
  <WhiteList>
    <Applications>
      <Application name="notepad++.exe"/>
    </Applications>
  </WhiteList>
```

The following table details the Application node highlighted above:

<table>
<thead>
<tr>
<th>Applications Attributes</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>name</td>
<td>The name of the application that can be trusted.</td>
</tr>
</tbody>
</table>
Restrict the file formats that can be protected

In the RMC_Classification.xml file, you can specify the file formats that can be protected using the context menu. If the file format is not listed under the Extensions label, user cannot right click and select the NextLabs > Protect option.

```xml
<Extensions>
  | .\.(txt|rtf|pdf|rh|dwg|doc[x]?)| (xls[x]?) | (ppt[x])$</Extensions>
```

Using Policies to List Classification Labels

Rights Management Client (RMC) supports policy obligations that specify the user profile name associated with the user logged in to RMC. This profile name corresponds to one of the Profiles node specified in the RMC_Classification.xml file.

In the NextLabs Policy Studio, you can write policies that are triggered based on the user. When such a policy is triggered, the user profile name indicated in the policy obligation determines which classification labels are displayed in the RMC user interface.

For more information about specifying appropriate profiles in the RMC_Classification.xml file, refer to Specifying the User Profiles.

Specify the User Classification Custom Obligation

Before you can create a policy which uses the User Classification custom obligation, you must ensure that your NextLabs Control Center’s configuration.xml file contains the following xml code:

```
<Obligation>
  <Display Name>Rights Management Classification Labels</Display Name>
  <Run At>PEP</Run At>
  <Name>OB_CLASSIFY</Name>
  <Arguments>
    <Argument usereditable="true">
      <Name>Group</Name>
      <Value default ="true">Default</Value>
    </Argument>
  </Arguments>
</Obligation>
```

For more details refer to, Configuring Rights Management Obligations.
The sample policy below indicates how you can configure the policy obligation to specify a set of classification labels based on the user attempting to view a file.

Note: The sample policy listed below enables the user to protect a file.

Sample Document Policy to Enable User Initiated Protection
The following Document Policy is triggered whenever a particular user (john tyler) attempts to view files from the classification resource.

Note: You must specify the policy Action as View if you want the policy obligation’s classification label set to display for the user.
The Custom Obligation check box is set and Rights Management Classification Labels is selected.

The Group field contains the name of the Profiles node (in your RMC_Classification.xml file). In the image above it is set to the Engineer profile. This is the same Profile that is included in your RMC_Classification.xml file as indicated below:

Note: If you do not specify a user profile for the Group field, then the Default user profile is used.

```xml
<Classify>
  <Profiles>
    <Default>0.1</Default>
    <Engineer>0.1</Engineer>
    <Product>0.1</Product>
  </Profiles>
</Classify>
```

When the user (john.tyler) attempts to view a file from this resource, Rights Management Client displays the classification labels (which have user ids 0 and 1) as indicated in the Engineer profile node of the RMC_Classification.xml file.
After you have configured your `RMC_Classification.xml` file (for more information, refer to Configuring your classification file) you must copy it to the `<RMS_DATA_DIR>` directory of your NextLabs Rights Management Server and then restart Tomcat.

For more information about the default `<RMS_DATA_DIR>` location, refer to the NextLabs Rights Management Server Administrator’s Guide.
After you have installed the Key Management Server, you should create a new shared key ring and generate a shared key. (This will not occur automatically.) The shared key will be sent to Rights Management Client on their next heartbeat.

Note: It is recommended that you setup a scheduled key rotation to ensure that the keys are not vulnerable from a security standpoint. Currently NextLabs Control Center does not support the ability to schedule encryption key rotation, therefore as the Administrator you must setup the key rotation schedule as a Microsoft Windows scheduled task.

The default key ring name is **NL_SHARE**.

Note: If you have distributed ICENet servers, you only need to generate Shared Key Rings and Keys on one host. Shared Keys and Key Rings will be automatically distributed across all ICENet servers locations where Key Management Server is installed.

Creating a Shared Key Ring and a Shared Key

NextLabs Rights Management Client encrypts user data using the Advanced Encryption Standard (AES) 256 bits. This section lists the steps involved in creating a new shared encryption key ring and key in the Key Management Server.

1. In the Command prompt on the device where Key Management is installed, change directory to `<Install Dir>\Nextlabs\Policy Server\tools\keymanagement`.

2. Run the following command to create a shared key ring (where the keyRingName is `NL_SHARE`):

   `keymanagement.bat -u <username> -w <password> -createKeyRing -keyRingName NL_SHARE`

3. Run the following command to create a shared key on the newly created key ring:

   `keymanagement.bat -u <username> -w <password> -generateKey -keyRingName NL_SHARE -keyLength 32`

The Shared Key must be 32 characters long. If you do not specify the `keyLength` value then the default length is 16 characters.
Where to Install Rights Management Components

Depending on your implementation, Rights Management components will need to be installed in different locations on your network. This section describes the Key Management Server and Rights Management Client.

**Key Management Server**

As is discussed in more detail in the Key Management section, Key Management is used to generate, delete, backup, and maintain keys and key rings used to encrypt files. Key Management can be performed from the server (Key Management Server, installed with NextLabs Control Center) or from the endpoint (Rights Management Client).

Key Management Server provides a centralized key store. Administrators can use it to create and maintain shared keys—keys that are shared across multiple users which allow encrypted files to be shared. Shared keys are automatically sent to endpoints upon the Policy Controller’s next heartbeat.

Key Management Server is installed with the Control Center platform, specifically, on the same host(s) where ICENet server is installed. If your NextLabs implementation includes multiple ICENet servers, Key Management Server should be installed with each. Key Management Server is necessary for creating and maintaining shared keys.

**Rights Management Client**

Rights Management Client is the tool that applies protection to files (in the form of encryption) at the endpoint. Rights Management Client must be installed on all endpoints where files will become protected and/or where protected files will be consumed (decrypted).
Rights Management Client installation also requires that the NextLabs Rights Management Server is already deployed and configured with the RMC_Classification.xml file. For more information about deploying the Rights Management Server and configuring the RMC_Classification.xml file, refer to the Rights Management Server Administrator's Guide.
Before you Install

Before you attempt to install and configure Rights Management Client (RMC) you must ensure that all of the following prerequisites have been met.

Network Requirements

You must ensure that the following firewall exceptions are defined for Rights Management Client:

- Outgoing heartbeat Traffic port: 8443

  Note: This port is configurable.

You do this in the Control Panel > Network Settings > Local Area Connection settings for each individual host.

These port exceptions are required to allow the RMC to send heartbeat messages to the NextLabs Rights Management Server, and receive policy bundles back from it; and also so the administrative applications can connect to the RMC for status updates and other information.

Note that these are all default port numbers, which you may have changed in your individual installation of Rights Management Server; if so, set the exception ports to the actual port numbers you have set.

Supported Platforms

Rights Management Client supports the following platforms and software:

- Microsoft Windows 7 (32 and 64-bit) and Windows 10 (32 and 64-bit)
- Adobe Reader X and XI
- Microsoft Office 2010 and 2013 (32 and 64-bit versions)

  Note: Rights Management Client supports stand alone as well as environments where both versions of Microsoft Office 2010 and 2013 are installed.

- SAP Visual Enterprise Viewer 8.0.3
- NextLabs Control Center (versions 7.6 and 7.7)
- NextLabs Rights Management Server 8.3

Supported CAD Applications

Rights Management Client supports Access Control on the following CAD applications:

- NX
- JT2Go
- Solid Edge
Creating your RMC Installation Package

The NextLabs Rights Management Client installation package is created using a Client Package Builder. In the Client Package Builder you can specify the Policy Server information as well as the type of operating system (and architecture) you want to install RMC on.

The Client Package Builder produces an xml file containing your configuration details and two versions of the appropriate installer. Both exe and msi versions can be used for performing silent installations while also supporting standard msi command line arguments.

1. Double-click the Client Package Builder installation file.

2. Review the terms and conditions of Installation, and click I agree.

3. Click Next.
4. Select the **Platform(s)** for which you want to create RMC installation packages.

![Platform and Language dialog]

5. Select the **Language** that you want to use as the default language for RMC.

*Note:* If the Rights Management Client (RMC) user is using a language that is not supported by RMC then the user interface is rendered in the language you have selected.

![Platform and Language dialog]

6. Click **Next**.
7. Type the Policy Server web service URL in the following format:

*Note:* The Policy Server web service URL is the address of your Rights Management Server web service URL.

https://<Your Rights Management Server URL>:<port number>/RMS/service

8. Enter the desired destination location where the configured RMC Installer package(s) is to be stored. Alternatively, you can click **Browse** and select an existing destination location.

*NOTE:* If you click **Browse** to select, the folder must have already been created before it can be selected here.

9. Select **Use Rights Management Server Login** if you want to use RMS to authenticate the login credentials. If you select this option, the *Default Domain* field appears. If you want to specify a default domain, enter the default domain. Otherwise, leave the field empty. If you do not select **Use Rights Management Server Login**, the application will use the default Windows login credentials.

10. Click **Next**.
11. Review the summarized configuration information and click **Finish** to build the Rights Management Client installation package.
Installing Rights Management Client Manually

The following steps demonstrate how to manually install Rights Management Client on your endpoint machine.

1. Double-click the NextLabs Rights Management Client.msi or.exe file.

2. In the installation wizard window, click Next.

3. Review and accept the terms of agreement, and then click Next.
4. Click Next.

*Note:* If you want to change the default installation location, then click *Change* and choose your new location.

5. Click Install.
6. Click Finish.
After you have installed the Rights Management Client (RMC) you must also ensure that you have enrolled all your users into Control Center.

If your users have not been enrolled in the NextLabs Control Center, they cannot be defined in the Policy Studio.

For more information refer to the Enrolling Users, Hosts & Apps chapter of the Control Center Quickstart Guide.

*Note:* Once your Rights Management Client is registered, you can configure certain parameters for your RMC using the Desktop Enforcer Profiles available in the NextLabs Control Center (Administrator console). For more details refer to *About Enforcer Profiles* in the NextLabs Control Center Administrator Guide.
Configuring the Rights Management Policy Model

If you plan on creating policies that apply Security Overlays, or enforce on different actions (Send, Clipboard, Screen Capture, Edit etc.), you must perform the configuration steps discussed in this section:

- Configuring Rights Management Obligations
- Configuring Rights Management Resource Attributes
- Configuring Special Actions

Configuring Rights Management Obligations

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 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 includes 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:

   [InstallDirectory]\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 will be 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 obligation to the policy, you will be able to supply parameters that specify what the obligation does.

Configuring Rights Management Resource Attributes

If you want to use specific custom attributes to base your policies on, you must perform the following steps to configure your Policy Studio user interface. Then you can use these custom attributes to display as drop down menu items in Policy Studio. You must configure these labels in the configuration.xml file.

Follow these steps to configure Rights Management Resource Attributes:
1. Use Notepad to open the product.xml file supplied by NextLabs support. This file includes all obligations, special actions, and resource attributes required for the NextLabs product.

2. Locate the <ResourceAttribute> sections 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 \[installDirectory]\NextLabs\Policy Server\server\configuration.

4. Locate the <CustomAttributes></CustomAttributes> section, and paste the obligations into the main configuration file.

5. Save the changes to the configuration.xml file and restart the NextLabs Control Center Policy Server service.

   *Note:* If your Control Center is deployed in a distributed topology then you must restart the Control Center service as well as the ICENet service on each machine.

After you complete this configuration and restart the NextLabs Control Center Policy Server service, the resource attributes are listed with their respective Display Names in the Policy Studio user interface (as properties that you can specify for a Resource).

You can then use these resource attributes to identify specific resources for your policy.

### Configuring Special Actions

Right Management has several special actions (Screen Capture, Clipboard, Classify, Send, and Decrypt). These special actions are not included by default in the installation of Policy Studio and must be manually configured before you can use them in policies.

Follow these steps to configure Rights Management Special Actions:

1. Use Notepad to open the file called product.xml. Contact NextLabs Support for the appropriate version of this file.

   *Note:* You can also refer to the xml code for each action as indicated in the Configuring the Rights section.

2. Locate and copy the special actions 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 <installDirectory>\server\configuration.

4. Locate the <ActionList></ActionList> section, and paste the special actions into the main configuration file.
5. Save your changes in the file and restart your NextLabs Control Center Policy Server service.

*Note:* Restart the NextLabs Control Center Policy Server service in the ICENet server.

After the system restarts, you test the configuration by opening Policy Studio and creating a New Action component. The new action should appear in the list of basic actions in the left side of the chooser.
Access and Usage policies govern what authorized users may do with protected content using the Rights Management Client.

Rights Management Client assumes the user does not possess any rights to perform any action. Therefore if you want to permit the user to perform any action (for instance decrypt a NXL protected document, perform a screen capture, or print a document) then you must write a policy that grants the appropriate rights.

This chapter explains Document Security Policies that control how documents are displayed and Enabling Users to Protect Files.
Security Overlays allow you to design policies that modify the appearance of documents when they are viewed. Security Overlays sit on the document window, rather than being embedded within a file, the way a standard Microsoft Word watermark works (for this reason, they can be used in addition to existing watermarks). Security Overlays are non-scrolling; they remain fixed on the screen even as viewers scroll through documents.

Security Overlays are viewed in applications supported by RMC.

RMC can display only one overlay at a time. It cannot display different overlays for different files opened at the same time.

Configuring Security Overlays

Before you can create a policy which uses the Security Overlay custom obligation, you must ensure that your NextLabs Control Center’s configuration.xml file contains the following XML code:

```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>
  </Arguments>
</Obligation>

<!-- Continued on the next page -->
```
Designing Access and Usage Policies

For more details refer to, Configuring Rights Management Obligations.

After you have configured the obligation for your Control Center deployment, you can use the custom obligation while creating policies in Policy Studio.
The following table lists the attributes which are included in the OB_OVERLAY custom obligation:

<table>
<thead>
<tr>
<th>Attribute</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Text**  | This is the text you want to display as the watermark. Supported variables: $(User) - shows the username; $(Host) - shows the machine name; $(Date) - shows the user login date; $(Time) - shows the user login time; 
| **Transparency** | Enter 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. |
| **FontName** | Enter the font name to display the watermark. The default font name is Sitka Text. |
| **FontSize** | Enter the font size to display the watermark. The default size is 36. |
| **TextColor** | Select a color to display the watermark. The default value is Black. |
| **Rotation** | Select the direction of rotation for your watermark. The default value is Anticlockwise. |

**What Actions Can Be Enforced Upon?**

Currently, Security Overlay policies can be designed to enforce only the View Rights on documents.

**Example Policy: View Security Overlay**

In our example, we design a policy that ensures any file labeled “Engineering IP” displays with a view overlay. The policy components for this example policy are:

*For Resource: Microsoft Office files and label “Engineering IP”*
*On Action: View*
*By Subject: All Users*
*Do: Allow, View Security Overlay Obligation*

**Create the New Policy and Define the Effect**

1. Select a folder and create a new policy within it. Select Document Policy for the Policy Type.

**Define the Policy Subject**

2. Define the Policy Subject. In our example, the policy should apply to all users, so we do not specify a User, Computer, or Application.
Define the Policy Action

3. With the policy tab selected, locate the Action for View and drag it into the Action field in the policy.

Define the Policy Resource

4. Add an existing Document Resource component for Microsoft Office files.

5. Click the + button and add a Document Resource component that references the label “Engineering IP.”

Note: In order for label values to display in a drop down menu item in Policy Studio, they must first be configured as a Resource Attribute in the Control Center configuration file prior to the above step.

6. Drag the Document component into the On Resources field in the policy.

![Figure 3-1: View Overlay Policy](image)

Define the Obligations, Submit and Deploy the Policy

7. If desired, supply an On Allow user alert explaining why the action may be denied.
8. In Select the Custom Obligation check box, and select **OB_Overlay** from the Name drop down menu. A list of settings display which determine the content and appearance of the overlay.

   ![Obligations](image)

   **Note:** The overlay is displayed with the current username and timestamp in the user’s application window. The time stamp is displayed in the Year/Month/Day/Hour/Minute/Second format.

9. Submit and Deploy the policy.

   When the policy enforces, the following overlay displays.

   ![Overlay Example](image)

   **Figure 3-2: View Overlay Example**
Enabling Users to Protect Files

NextLabs Rights Management Client assumes that out of the box, all users have no rights to protect files. If you want a user or user group to be able to use RMC to protect a document then you must deploy a policy that allows the View Action for a user and triggers the classification obligation.

A sample policy that enables a single user to protect a document is listed in the Sample Document Policy to Enable User Initiated Protection section.
Applying Protection

How Do Protected Files Behave?

Rights Management Client (RMC) assumes the user does not possess any rights to perform any action. Therefore if you want to permit the user to perform any action (for instance decrypt a NXL protected document, perform a screen capture, or print a document) then you must write a policy that grants the appropriate rights. In short, what a user can do with a NXL protected document depends on the rights the user has been granted through policies.

Encryption can be applied to files via any machine that has RMC installed and running on it. Users may classify documents based on the tags made available in the RMC by the Administrator.

For more information about configuring classification tags in the RMC, refer to Configuring your classification file.

Only authorized users on machines with RMC installed and running on them are able to view these encrypted files.

Protected files are indicated by a blue icon (refer to the image below).

Note: Rights protection done in version 7.1 (or earlier versions) of Rights Management is not compatible in the current version. If you are switching from any of these earlier versions of Rights Management then your existing files will no longer be detected by the policy. Rights protection done using version 7.5 and above is supported.

Removing Protection or Reclassifying

Only authorized users are allowed to remove protection or reclassify a NXL protected document. If the user does not have the rights to remove protection or reclassify the file then this option is disabled for the user.
Introduction

This chapter describes administrative procedures associated with Rights Management. Information is broken into the following sections:

- Key Management
- Monitoring Rights Management Clients
- Collecting Logs
- Viewing Activity Logs
- Upgrading from RMC 8.0 or later
Key Management

Key Management is used to generate, delete, backup, and otherwise maintain the keys and key rings used for NextLabs Encryption. Key Management includes Key Management Server installed with the Control Center (on the same device as the ICENet server). The Rights Management Client syncs with the NextLabs Control Center and uses the keys from the Key Management Server to encrypt files.

Note: For more information on installing Server and Endpoint Key Management, see Setting Up Rights Management Client.

This section provides instructions for managing encryption keys using the Key Management utility. Information is broken into the following sections:

- Managing Keys
- Server Key Management
- Key Management Passwords

Managing Keys

The Key Management utility on the Control Center (keymanagement.bat) should always be used to generate and maintain shared encryption keys and key rings. Keys created using Server Key Management are automatically sent to Rights Management Clients on their next heartbeat. In addition to creating new keys and key rings, you should perform all other administrative procedures involving key rings at the Control Center (export, delete, and so on). All shared keys must be generated manually (none will default upon installation of Server Key Management).

![Adding a Key to NL_SHARE](image)

Figure 5-1: Creating an Encryption Key (NL_SHARE)
This section describes how to access the Server Key Management utility, how to use it to perform different key management procedures, and provides additional information on selected procedures and best practices.

Key Management may be installed in different locations depending on your implementation.

Note: In a distributed environment, Key Management utility must be installed on the same machines as the ICENet servers.

You can run the keymanagement.bat utility on a different host than where Key Management is installed (for example, you can run the utility from the same host as the Policy Server and target the ICENet host). In this case, you must specify the location of the Key Management Server (see instructions below).

Note: If you have Key Management Server installed in multiple locations, you only need to create the shared key ring and key once. It will be distributed automatically.

Using the Server Key Management Tool

To access the Server Key Management utility, follow these steps:

1. In the Command prompt on the device where Key Management is installed, change directory to \Nextlabs\Policy Server\tools\keymanagement.

2. The basic command for running key management is as follows:

   keymanagement.bat [-s <server>] [-p <port>] -u <username> -w <password> <additional arguments>

In this command,

- `-s <server>`: the server host name. The default is localhost. If you are running the command on the same host where Server Key Management is installed, this entry is optional. If you are running this command from another location (i.e., the host where the Policy Server is installed), the server name must be included here.

- `-p <port>`: the server port. This entry is optional and the default is 8443. If you are running the command on the same host where Server Key Management is installed, this entry is optional. If you are running this command from another location (i.e., the host where the Policy Server is installed), the server name must be included here.

- `-u <username>`: the user name. This is the Administrator defined during the setup of the Control Center.

- `-w <password>`: the password. This is the Administrator password defined during the setup of the Control Center. If this is not supplied, you will be prompted to enter it before the command executes.

- `<additional arguments>`: see the table below for available arguments.
Note: If you run this command without supplying any arguments, a help screen will display with usage examples.

Using the Server Key Management Tool

The table below lists all the arguments you supply to perform different Key Management procedures. All commands listed below are case sensitive, except for Key Ring Names. Even if a Key Ring Name is typed in mixed or lower case, it is converted to all Upper Case.

Note: Server Key Management arguments do not need to be typed in the same order as they display in the following table.

Server Key Utility

<table>
<thead>
<tr>
<th>Procedure</th>
<th>Command</th>
<th>Explanation and Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td>Create a new key ring</td>
<td>keymanagement.bat -createKeyRing -keyRingName NL_SHARE</td>
<td>Creates a new key ring, named NL_SHARE. This is the name of the shared key ring that defaults on endpoints.</td>
</tr>
<tr>
<td>Generate a new key</td>
<td>keymanagement.bat -generateKey -keyRingName &lt;KEY_RING_NAME&gt; [-keyLength &lt;length in bytes&gt;]</td>
<td>Generates a new key on the key ring &lt;KEY_RING_NAME&gt;. Key Ring Names are always converted to all upper case. The -keyLength command is optional. It can be supplied to create a key of a different length than the default of 16 bytes. The procedure for performing a key rotation is the same as generating a new key on an existing key ring (see More About Performing Key Rotations from the Server).</td>
</tr>
<tr>
<td>List key rings</td>
<td>keymanagement.bat -listKeyRing</td>
<td>Outputs a list of existing key rings</td>
</tr>
<tr>
<td>List keys on a key ring</td>
<td>keymanagement.bat -listKey -keyRingName &lt;KEY_RING_NAME&gt;</td>
<td>Outputs a list of keys associated with a named key ring, including the index number and key hash.</td>
</tr>
<tr>
<td>Back up (export) a key ring</td>
<td>keymanagement.bat -export -keyRingName &lt;KEY_RING_NAME&gt; -file &lt;File_Name&gt; -filePassword &lt;Password&gt;</td>
<td>Exports the named key ring to a specified file name. It will be password protected with the password supplied in the command. If the -filePassword command is omitted, you will be prompted to enter a password before the command executes. (See More About Backing up a Key Store.)</td>
</tr>
<tr>
<td>Back up all key rings</td>
<td>keymanagement.bat -exportAll -folder &lt;folder name or path&gt; -filePassword &lt;Password&gt;</td>
<td>Exports all key rings to a specified location. The folder must already exist. Each Key Ring will be exported as a single file that is password protected with the password supplied in the command. If the -filePassword command is omitted, you will be prompted to enter a password before the command executes. The files will be given the extension &quot;.keyring.&quot; This same extension must be used to import the key ring.</td>
</tr>
</tbody>
</table>
More About Performing Key Rotations from the Server

Keys must be created manually at the Control Center so they can be deployed to all registered Rights Management Clients upon the next heartbeat.

It is recommended that you set up a Key rotation schedule to ensure that the keys are not vulnerable from a security standpoint. Currently NextLabs Control Center does not have the ability to schedule encryption key rotation therefore, you must setup a rotation schedule as a Windows Server scheduled Task.

More About Backing up a Key Store

It is a recommended that every time you perform a key rotation, you back up the encryption key ring. That way, in the event of a system failure or other catastrophic event in which an encryption key is lost, you can import the key ring from the backup folder, and still access encrypted data.

Key Management Passwords

There are three kinds of passwords that Administrators need to be aware of as they perform Key Management procedures.

Control Center Administrator Password: This is the Administrator password that is designated during the initial installation of the Control Center. Users will need to supply this password in order to run most Key Management commands (see Server Key Management).
Control Center Encryption Key Store Password: This is the password defined in the installation wizard while installing the Key Management Server. This password is necessary for accessing the key store within the Control Center. Once defined, this password is embedded in the Policy Server’s configuration.xml file and used for several back-end processes. Once this password is lost, it cannot be recovered and will have to be reset.

Exported Key Ring Passwords: Whenever Administrators export key rings for backup purposes, they can encrypt the backup file by supplying a password. This password must be supplied to import the key ring.

Note: If you need assistance in either recovering or resetting passwords, contact NextLabs support.
Monitoring Rights Management Clients

You can monitor the status of all Rights Management Clients in the network, by opening the NextLabs Control Center Administrator, going to the Status tab, and clicking the Policy Enforcer Status link. By default, this tab displays the status of all enforcers in the system that are displaying warnings. To show all enforcers with or without warnings, uncheck the Enforcers with Warnings Only checkbox (A).

**Note:** The RMC status is displayed under the Desktop Enforcer.

To view only desktop enforcers, select *All Desktop Enforcers* from the Show combo-box list at the left (B). If you are interested in the status of enforcers on a specific enforcer host or host group, you can also filter by host name by typing it into the Search By Host field (C) and clicking the Search button.

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>Indicates the current status of this enforcer, which may be either of the following: Green light = Clear: the policy enforcer is sending normal heartbeats. Exclamation point = Warning: the policy enforcer has not sent a heartbeat in the last 24 hours.</td>
</tr>
<tr>
<td>Host</td>
<td>Name of the machine where the policy enforcer is installed.</td>
</tr>
<tr>
<td>Type</td>
<td>Indicates the policy enforcer type: File Server Enforcer or Desktop Enforcer.</td>
</tr>
</tbody>
</table>
### Information on Policy Enforcer Status (Continued)

<table>
<thead>
<tr>
<th>Column</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Heartbeat</td>
<td>Time stamp of the last heartbeat generated by this policy enforcer. If the policy enforcer is running normally, this time should correspond to the configured heartbeat interval. However, keep in mind that this does not necessarily indicate a problem, since certain policy enforcers—in particular, those on laptop computers used by remote personnel or computers that are turned off when not in use—might not be able to send a heartbeat for an extended period of time even though they are operating normally.</td>
</tr>
<tr>
<td>Last Policy Update</td>
<td>Tells when a new or modified policy or policy component was last deployed to this policy enforcer.</td>
</tr>
<tr>
<td>Policy Up to Date</td>
<td>A check mark appears if the policy enforcer has received the latest version of the policies that are targeted for deployment to it.</td>
</tr>
<tr>
<td>Profile Name</td>
<td>Tells which policy enforcer profile is assigned to this host. This profile determines behavior such as logging and heartbeat frequency.</td>
</tr>
<tr>
<td>Hide</td>
<td>Click to remove this host from the display. This is useful when the policy enforcer software has been uninstalled, and you therefore no longer need to monitor that host. If a policy enforcer is ever reinstalled on this host, the host will reappear on the list. If you click Hide by mistake on a host with an active policy enforcer, it will reappear automatically the next time the policy enforcer sends a heartbeat.</td>
</tr>
</tbody>
</table>
Collecting Logs

There may be times when administrators need to know how policies are being enforced (or not enforced) in accordance with user actions for troubleshooting or diagnostic purposes. NextLabs provides a support utility that allows you to retrieve the decrypted bundle and agent logs that can help you troubleshoot such issues better.

Rights Management Client also includes the ability to collect debug logs for itself.

Enabling Debug Logs

1. In the System Tray, right-click the RMC icon.
2. Select Enable Debug.

Collecting Debug Logs

After logging is enabled, recreate the user behavior in order to capture it, and then collect debug logs. The following steps indicate how you can collect the Debug Logs:

1. In the System Tray, right-click the Rights Management Client icon.
2. Select Collect Debug Logs.

Note: The Debug Logs are saved as a zip file on your Windows desktop.
Viewing Activity Logs

RMC generates activity logs that captures events blocked by the application when a user performs any action without rights. This is useful for the management to view the user actions blocked by the application.

The audit database is located in the following directory:

\<RMC_INSTALL_DIR>\profiles\<USER_SID>\audit.db

In order to view the log files, you must export the database contents to a log file as shown below.

1. Open the Command Prompt.
2. In the Command Prompt, go to the \<RMC_INSTALL_DIR>\bin directory.
3. Run the following command to export logs from audit.db to a log file:

   nxrmconv.exe export activitylog c:\test\a.log.

   Note: You must create the “test” directory before you export.
Upgrading from RMC 8.0 or later

If you are upgrading from Rights Management Client 8.0 or later, simply run the 8.3 installer to upgrade your machine.

You can also configure NextLabs Rights Management Server to host the latest Rights Management Client installer. Each instance of Rights Management Client registered with your Rights Management Server automatically upgrades to the latest version which you have configured on the Rights Management Server.

*Note:* The Rights Management Client Auto Update feature requires the NextLabs Rights Management Server is already configured to host the latest Rights Management Client installer. For more information, refer to the *Configuring Client Management Settings* section in the NextLabs Rights Management Server Administrator’s Guide.
Rights Management for JT2Go

This chapter covers the following sections:

- About Rights Management for JT2Go
- Before you Install
- Installing Rights Management Client for JT2Go
About Rights Management for JT2Go

NextLabs Rights Management for JT2Go is a web-based solution that enables users to apply rights-protection to JT files. It is a secure viewer that provides a zero-client CAD viewing capability for JT files.

Rights Management Client does not support the following features for JT2Go:

- Rights-protection on a JT file
- Classification of the document
- Removing Protection

The JT files can be protected using Rights Management Server. See the NextLabs Rights Management Server Online Help for applying rights-protection to a JT file. In order to view a JT file, log into RMC and double-click a JT file. Based on the access rights, you can see the JT file with overlays. The print option is disabled.
Before you attempt to install and configure Rights Management Client (RMC) for JT2Go, you must ensure that all of the following prerequisites have been met.

**Supported Platforms**

Rights Management Client supports the following platforms and software:

- Microsoft Windows 7 (64-bit) and Windows 10 (64-bit)
- JT2Go version 11.2 and above
- NextLabs Control Center (versions 7.6 or 7.7)
- NextLabs Rights Management Server 8.3
The following steps demonstrate how to manually install Rights Management Client on your endpoint machine.

1. Double-click the `setup.exe` file

2. In the installation wizard window, click **Next**.

3. Review and accept the terms of agreement, and then click **Next**.
4. Click **Next**.

*Note:* If you want to change the default installation location, then click **Change** and choose your new location.

5. Click **Install**.

6. Click **Finish**.