NilRead rejection notes

If a study, series or image is deleted from the NilRead server, a rejection note is created with a list of the rejected (deleted) instances. Rejection notes are used to notify remote servers to delete these rejected instances. You can configure which remote servers receive NilRead rejection notes.

Rejection notes are created in the following scenarios:

- a user deletes a study from the Patient Study Directory
- a user edits a study and deletes the original study
- a user deletes a series from a study
- a user deletes an image from a study

By default, rejection notes generated by NilRead use the following title:

(113039, DCM, "Data Retention Policy Expired")

Received rejection notes

NilRead can also accept rejection notes from remote servers. If a study, series or image is deleted on a remote server and NilRead receives a rejection note, the rejected instances will be deleted on the NilRead server as well.

Configure IOCM settings

1. Select **Settings**.
2. Under **Devices**, select **IOCM**.
3. Enter the following information, then select **Save**.
   - **Enable** Allow NilRead to send and receive rejection notes. If this option is disabled, NilRead will not create rejection notes. NilRead will still receive rejection notes from remote servers but the notes will not be applied.
   - **Accept rejection notes from** Select the types of sources that NilRead will accept rejection notes from.

- **Send Nil rejection notes to** Select the remote application entities (AE) that NilRead will send rejection notes to.
- **Generate rejection notes when delete** You can choose to create rejection notes when a study is deleted (**Study**) and when a series or images is deleted (**Series/instances**).
- **Keep rejection notes for XX days** Number of days to keep rejection notes. Notes older than the retention period will be deleted the next time a scheduled data purge occurs. To remove older notes immediately, select **Purge** at the bottom of the page.

The **Rejection Notes** list contains the notes NilRead has sent and received. Rejection notes received from a remote server are applied automatically (check the timestamp in the Applied column to verify that a note has been applied). To apply a rejection note immediately, select the note, then select **Apply**. To delete a rejection note, select the note, then select **Delete**.

NilRead ignores all instances that have been rejected. If the rejected instances must be reimported, delete the corresponding rejection notes and resend the rejected instances to NilRead.

> **Note**
> Rejection notes are also shown on the **DICOM Activity** page.

Manage users

About user privileges

ADMINISTRATORS ONLY

You can manage NilRead user privileges at several levels. This allows you to tightly control user access to NilRead features and the Patient Study Directory. A user's privileges are initially based on their role and group assignment; these are both assigned in the user's account. The user's privileges can then be customized through their account.

> **Note**
> Users must be assigned the StudyListAccess privilege in order to access the Patient Study Directory. For details, see **Privilege descriptions**.

Role

Users are assigned default privileges based on their role (Admin, User or Guest). This role is assigned in the user's account.

- **Administrators** typically have full privileges for NilRead use and configuration; only Administrators can manage NilRead users. By default, Administrators have full privileges.
- **Users** are regular NilRead users. Users typically have access to the entire Patient Study Directory.
- **Guests** are occasional NilRead users, such as external referring physicians. Guests can typically only see studies for their own patients. Guests can access emergency override ("break glass"). By default, Guests have no privileges.

For more information, see **Manage user accounts**.

Group

Users are also assigned the default privileges of the group to which they belong. This group is assigned in the user's account. For details on setting up groups, see **Manage user groups**.

Account

User privileges can be customized in the user's account. The default privileges inherited from the user's role and group can be changed and additional privileges can be assigned. For more information, see **Manage user accounts**.

Profile

Administrators can manage their privileges using their profile. **Guests** and **Users** can only change settings such as their name, email address and password. For more information, see **Manage your user profile**.

Privilege descriptions

ADMINISTRATORS ONLY

The following privileges can be assigned to a group or user.

- **Assets** Manage site-level assets.
- **AssignWorkItems** Assign work items to other users and groups. Make work items public.
- **AutoEnroll** Automatically create NilRead user accounts for members of a Windows group on their first login.
- **BookmarkSaveSend** Create and share a bookmark. Note: The user must also have the SaveEvidence privilege and the EnableSaveMenu configuration option must be set to true.
- **Collaboration** Access collaboration tools.
- **ContentDownload** Download DICOM files. Note: The user must also have the GuiPatient privilege in order to access the Download option in the image viewer context menu.
- **ContentUpload** Upload DICOM files.
- **CreateAccounts** Create, modify, and delete NilRead user accounts.
- **CreateSecureLinks** Create and send secure study links.
- **DicomClearLogs** Remove logs from the DICOM Activity page (see **Monitor DICOM patient study transfers**).
- **DicomConfig** Manage DICOM services (see **Manage DICOM services**). Note: The DICOM Activity button is only enabled if the patient directory provider implements the **IDicomPatientDirectoryProvider** interface.
- **DicomConfigEdit** Edit DICOM configuration.
- **DicomDelete** Delete saved presentation state information. Note: The user must also have the GuiPatient privilege in order to access the Delete Image option in the image viewer context menu. The user must also have the SaveEvidence privilege in order to delete persistent curved reformat centerline data.
- **DicomPrint** Manage DICOM printers.
- **DicomQueryRetrieve** Access the Search tab in the Patient Study Directory and retrieve patient studies from a DICOM server (see **Retrieve studies to the local database**). Note: The DICOM Activity button is only enabled if the patient directory provider implements the

IDicomPatientDirectoryProvider interface.

- **DicomRT** Enables protocol support and tools for DICOM RT studies.
- **DicomStore** Access the DICOM store features. Note: The DICOM Activity button is only enabled if the patient directory provider implements the IDicomPatientDirectoryProvider interface.
- **EditAnonTemplates** Create, modify, and delete anonymization profiles and masks.
- **EditHangingProtocols** Create, modify, delete and enable/disable user hanging protocols.
- **EditPatientStudy** Edit patient-level and study-level DICOM attributes. Note: The Edit Image Header option requires the ImageHeaderEditorEnabled configuration setting to be set to true.
- **EditSystemHangingProtocols** Create, modify, delete and enable/disable system hanging protocols. Note: The user must also have the EditHangingProtocols privilege.
- **EditWorkItems** Create, modify and delete worklists and folders.
- **EmergencyOverride** Use emergency override ("break glass") to access patient studies (see **Use "Break Glass" to find studies**). NilRead guest users typically have limited access to the Patient Study Directory. However, guests may be given access to emergency override ("break glass") which allows them to search for studies based on patient name and study accession number. For example, a referring physician may only have access to studies containing his own name. If the referring physician's name is misspelled or missing from a study, he will be unable to access the study using the Patient Study Directory. However, the referring physician can search for the study if he has been granted the emergency override privilege.
- **EmergencyOverrideRestrictedContent** Use emergency override ("break glass") to view XDS content.
- **FhirAccess** Provides read-only access to FIHR patient and imaging study resources. Allows the user to acquire access tokens from the NilRead token endpoint and query patient information on the patient endpoint.
- **FhirConfig** Edit FHIR configuration.
- **FhirUpdate** Modify patient information using the patient endpoint with the access token.

- **GuiAdvanced** Access all user interface features. (The user's role and privileges may limit the features they can view.)
- **GuiBasic** Access basic user interface features. Only a single study can be reviewed in the image viewing area. Advanced features, such as measurement tools and hanging protocols, will not be available. (The user's role and privileges may limit the features they can view.)
- **GuiIntermediate** Access intermediate user interface features. For example, basic measurement tools, screen layouts and cross-correlation between series are available. Multiple studies can be reviewed in the image viewing area at the same time. Advanced features, such as advanced measurement tools and hanging protocols, will not be available. (The user's role and privileges may limit the features they can view.)
- **GuiPatient** Access simple user interface features. Intended for patient use. Note: This privilege cannot be applied to administrator users or members of administrator groups.
- **IOCM** Edit IOCM configurations.
- **LifecycleManagement** Enable and modify data lifecycle options (see **Manage data lifecycle policies**). Enable and modify prefetch option (see **Manage prefetch settings**).
- **MprProtocols** View MPR views.
- **OverrideLosslessModalities** This privilege has been replaced by the AlwaysLosslessModalities configuration setting. Previously, this privilege allowed a user to override system settings that specify that images from specific modalities are always shown as lossless, uncompressed images.
- **PatientDirectory** View all studies in the local database.
- **PersistentAnnotations** Allow persistent annotations and measurements across review sessions.
- **RestrictedSiteAccess** Access sensitive data on restricted sites.
- **SaveEvidence** Save presentations and key images. Save secondary capture images (the user must also have the SecondaryCaptureCreation privilege). Save bookmarks (the user must also have the BookmarkSaveSend privilege and the EnableSaveMenu configuration option must be set to true). Print images from the image viewer. Access the Link option in the image

viewer context menu. Access the Axial, Coronal, and Sagittal options in the MPR Views menu. Access the 1+1 and 3D Only options in the 3D Views menu. Generate, save, and delete persistent curved reformat data (the user must also have the DicomDelete privilege).

- **SecondaryCaptureCreation** Create secondary capture images (see **Share secondary capture images**). Note: The user must also have the SaveEvidence privilege.
- **ShowBookmark** Display a list of bookmarks in Presentations (see **Use presentations**).
- **SkypeIntegration** View Skype controls in the Collaboration panel. Note: The SkypeEnabled configuration option must also be set to true.
- **Spinemapper** View Spine Layout views.
- **StudyListAccess** Access the Patient Study Directory from the directory and the image viewer.
- **StudyNoteCreation** Create study notes.
- **ThreeDProtocols** View 3D views.
- **VesselAnalysis** Access Vessel Analysis views.
- **VesselTrace** Access the Vessel Trace tool. Note: The user must also have the ThreeDProtocols privilege.
- **ViewAnalytics** View Analytics (see **View analytics**).
- **ViewPublicWorkItems** Access public (unassigned) worklists and folders created by administrators.
- **ViewRestricted Content** View restricted content from XDS repositories.
- **XdsAccess** Access XDS repositories.

Manage user groups

ADMINISTRATORS ONLY

You can use groups to assign NilRead privileges to users (see **Privilege descriptions**). If NilRead is part of a domain, you can also add Active Directory groups to NilRead. If changes are made to an Active Directory group, such as adding users, the changes are automatically applied in NilRead as well.

Note
You can also manage privileges for individual users (see **Manage user accounts**).

Access group settings

1. Select **Settings**.
2. Under **User Management**, select **Groups**.

See the next sections for details on managing groups.

Create an application group

An application group is specific to NilRead and is not linked to an Active Directory group.

1. In the **Group** field (below the **Application Groups** area), enter the group name.
2. Select **Create**.
3. Select the type of group (Admin or User).
4. The **Granted Privileges** area lists the default privileges assigned to the group. By default, User groups have basic privileges (such as accessing the Patient Study Directory) and Admin groups have full privileges. To add or remove privileges from the group:
   - **Add a privilege** Select a privilege in the **Revoked Privileges** area, then select **Grant**.
   - **Remove a privilege** Select a privilege in the **Granted Privileges** area, then select **Revoke**.
5. In the **Session Timeout** field, select the session timeout period. A user's session will end if they are inactive for this amount of time.

Add an AD group to NilRead

You can add Active Directory groups to NilRead.

1. In the **AD Groups** area, select a group, then select **Add**.
2. Enter the following information, then select **OK**.
   - **Name** Name of the LDAP server.
   - **URL** URL for the LDAP server.
   - **Username**, **Password** Credentials for connecting to the LDAP server. Leave blank to connect using the credentials of the IIS application pool.
   - **Simple Bind** Use simple bind authentication when connecting to an LDAP provider. Typically used with ADAM and other non-Microsoft servers.
   - **SSL** Use a secure connection when using simple bind authentication.
3. In the **CN** field, enter the name of the Active Directory group you want to add, then select **Search**. Groups matching your search criteria are shown in the **AD Groups** area.
4. In the **AD Groups** area, select the group you want to add, then select **Add**. The group is added to the **Application Groups** area.
5. The **Granted Privileges** area lists the default privileges assigned to the group. To add or remove privileges from the group:
   - **Add a privilege** Select a privilege in the **Revoked Privileges** area, then select **Grant**.
   - **Remove a privilege** Select a privilege in the **Granted Privileges** area, then select **Revoke**.

Edit or delete a group

1. In the **Application Groups** area, select the group, then select **Delete**.
2. In the **AD Groups** area, select the group, then select **Remove**.
3. Select **Edit**. Modify the details, then select **Save**.

   or

   Select **Delete**.

Manage user accounts

ADMINISTRATORS ONLY

A user account defines the NilRead user's username, role, and group assignment. The user's privileges are shown in the user's account and can be modified. You can also lock user accounts and reset user passwords.

> **Note**
> Users can manage some of their account information through their profile (see **Manage your user profile**).

1. Select **Settings**.
2. Under **User Management**, select **Accounts**. Existing NilRead user accounts are shown.
3. If you have included Active Directory groups in NilRead, select **Refresh** to update the **Accounts** tab with any changes to Active Directory user accounts.

See the next sections for details on managing user accounts.

Add an account

1. Select **Add**.
2. In the **Account** area, enter the user's information.
   - **User Name** Username to login to NilRead.

     > **Note**
     > The user receives an automatic email with their NilRead password when their NilRead user account is created.

   - **Role** NilRead role (Admin, User, Guest). By default:
     - Guests have no privileges.
     - Users have basic privileges, such as accessing the Patient Study Directory.
     - Administrators have full privileges. Only Administrators can manage users.
   - **Email** Email address.
   - **Skype ID** Skype ID. Allows the user to participate in Skype sessions.
   - **Phone** Phone number.

- **Facility, Department, Job Description** User's facility and job information.
- **Notify on Study Arrival** User will receive an email when a new study containing one of the user's DICOM person name matches is added to the database.
- **Last Name, First Name, Middle Name, Prefix, Suffix** User's name.
- **Password** Password to login to NilRead.
- **Expiry Date** Date the user's access to NilRead will expire.
  - Select  and select an expiry date. Select whether the user's account will be locked or deleted on the expiry date.
  - Select  to remove the expiry date and set the user's access to **Unlimited**.

3. (Optional) In the **Groups** area, select the group to which the user belongs. Guests cannot be assigned to groups.
   - **Add a user to a group** Select a group in the **Not Member** area, then select **Add**.
   - **Remove a user from a group** Select a group in the **Members** area, then select **Remove**.
4. The privileges assigned to the user are shown in the **Privileges** area (see **Privilege descriptions**). These privileges are initially based on the user's role and group but can be modified.
   - **Grant a privilege to a user** Select a privilege in the **Revoked** area, then select **Grant**.
   - **Remove a privilege from a user** Select a privilege in the **Granted** area, then select **Revoke**.
5. Select **OK**.

Edit or delete an account

1. Select the user account. To find an account, enter account information in the blank row at the top of the tab.
2. Select **Edit**. Modify the details, then select **Save**.
   or
   Select **Delete**.

Lock an account

1. Select the user account. To find an account, enter account information in the blank row at the top of the tab.
2. Select **Lock**. The user's Locked status changes to True.
3. To unlock an account, select **Lock**. The user's Locked status changes to False.

Reset a user's password

If you reset a user's password, the user will receive an email with a new auto-generated password.

1. Select the user account. To find an account, enter account information in the blank row at the top of the tab.
2. Select **Reset**.

Manage NilRead

Customize the navigation tree

ADMINISTRATORS ONLY

By default, the navigation tree in the Patient Study Directory shows only worklists and folders that are public or belong to the current user.

You can add worklists and folders belonging to specific groups and users to the navigation tree, making these items available to all NilRead users.

1. In the Patient Study Directory, select  above the navigation tree.
2. Select groups and users. All NilRead users will be able to view the worklists and folders for these groups and users.
   - **Groups** To add groups, select one or more groups in the **Hidden** area, then select **Show**. To hide groups, select one or more groups in the **Shown** area and select **Hide**.
   - **Users** To add users, select one or more users in the **Hidden** area, then select **Show**. To hide users, select one or more users in the **Shown** area and select **Hide**.
3. Select **OK**.

Set up review folders

ADMINISTRATORS ONLY

NilRead users can use folders to track whether studies have been reviewed. A typical example is to group studies that require review in a **For Review** folder, then move these studies to a **Reviewed** folder once they have been reviewed. For more information, see **Track review status**.

In order to set up the review workflow, you must create the review folders and add folder icons to the image viewer toolbar. See the next sections for details.

Create review folders

Create the folders used to review studies (such as **For Review** and **Reviewed**) and grant access to these folders to authorized users. Note that you can use more than two folders for the review process and can use any name for the folders. For details on creating folders, see **Manage folders**.

Create review folder toolbar icons

Create icons for the review folders on the image viewer toolbar. Users will be able to use these icons to easily move studies from one folder to another.

1. Select **Settings**.
2. Under **System**, select **Third Party Applications**.
3. For each icon, select **Add** and enter the following settings.
   - **Application** Icon label.
   - **Target** Select **API**.
   - **Method** Select **POST**.
   - **Shortcut** (Optional) Keyboard shortcut to launch a third-party application or make a web API call.
   - **Launch URL** URL to launch the NilRead web API:
     `api/nil/relay/$token$/nil-move-study/$vp$`
   - **Data** API parameters that define the source and destination folders. For example:
     "For Review" folder:

```
{"fromItemId":"1159","toItemId":"1158"}
```

"Reviewed" folder:

```
{"fromItemId":"1158","toItemId":"1159"}
```

- **Icon URL** Icon images to indicate the study state (in the folder and not in the folder). The following icons are provided:

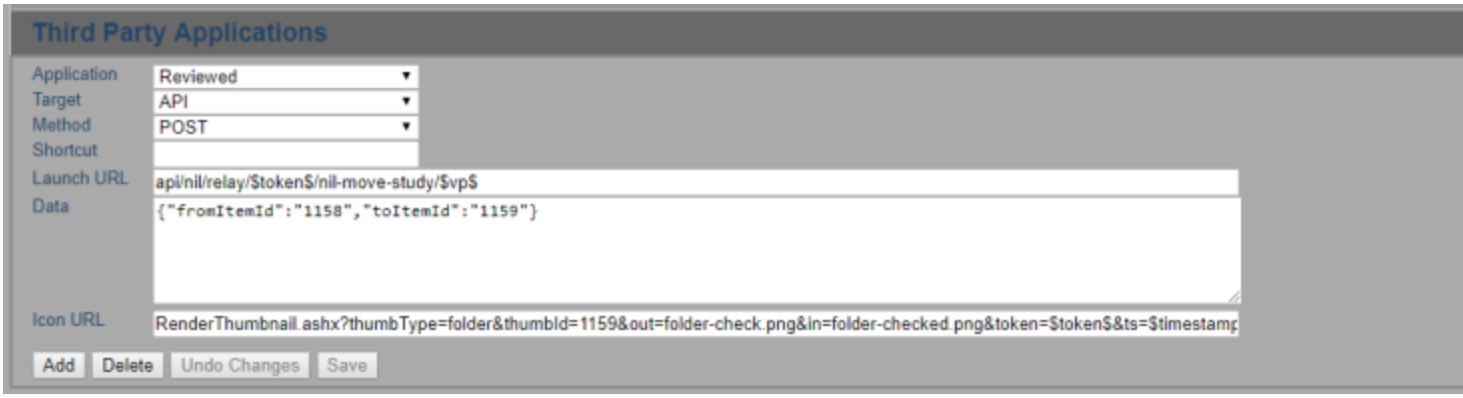
  "For Review" folder:

  ```
  RenderThumbnail.ashx?thumbType=folder&thumbId=1158&out=folder-add.png&in-
  n=folder-added.png&token=$token$&ts=$timestamp$
  ```

  "Reviewed" folder:

  ```
  RenderThumbnail.ashx?thumbType=folder&thumbId=1159&out=folder-check-
  .png&in=folder-checked.png&token=$token$&ts=$timestamp$
  ```

The following example shows two toolbar icons (Review and Reviewed) that allow users to move studies between two folders.



4. Select **Save**.

Manage patient search results

You can set the maximum number of studies that are returned on the Patient Search page in the Patient Study Directory.

1. Select **Settings**.
2. Under **Devices**, select **DICOM**.
3. In the **Patient Search** area, click **Edit**.
4. Enter the maximum number of query results, then click **Save**.

Manage secure study links

ADMINISTRATORS ONLY

Secure link settings

You can select the available security options that users can choose when sending secure study links (see **Send secure study links**). You can customize these settings for each site.

1. Select **Settings**.
2. Under **System**, select **Shared Links**.
3. Select the security options that users can select when sending a study link, then select **Save**.

Email Options