NERC

NORTH AMERICAN ELECTRIC RELIABILITY CORPORATION

ERO Enterprise User Guide for the Secure Evidence Locker (SEL) Analysis Environment and Documentum D2

Version 1.1
March 17, 2021

Armedia
Armedia, LLC
8221 Old Courthouse Road
Suite 300
Vienna, VA 22182

Contents

Document History

Name	Date	Reason for Changes	Version	Approval
Armedia	11/17/2020	Initial draft	0.1	
Armedia	12/22/2020	Updated to separate portal information in a separate guide	2.0	

Glossary

Acronym/Term	Description
ACL	Access Control List. Permission set for an object…who (user groups & users) can do what (permissions).
BOF	Business Object Framework
Cabinet	An area within the repository which is designated to a specific region.
CEA	Compliance Enforcement Authority
CIP	Critical Infrastructure Protection
CMEP	Compliance Monitoring and Enforcement Program
CN	Canonical Name
CSV	Comma Separated Values (refers to the manifest that will be created as part of each submission)
Documentum	An enterprise content management platform, now owned by OpenText.
ECM	Enterprise content management. A set of processes and technologies which manage information flows across the organization—from capture through to archiving and disposition.
ERO	Electric Reliability Organization
FERC	Federal Energy Regulatory Commission
ICAP	Internet Content Adaptation Protocol
LDAP	Lightweight Directory Access Protocol
Lifecycle	A lifecycle is a set of states that define the stages in an object’s life.
Locker	Locker, short for Secure Evidence Locker (sometimes referred to as the repository)
Metadata	Structured data which describes the content item. Metadata is ‘data about the data’. The content metadata is shown on the Properties panel in Documentum D2.
MRO	Midwest Reliability Organization (Regional Entity)
NCR	NERC Compliance Registry Identification Number (ID)
NPCC	Northeast Power Coordinating Council (Regional Entity)
NERC	North American Electric Reliability Corporation
OU	Organization Unit
O&P	Operations & Planning

PNC	Potential Non Compliance
Records Management	System used to control NERC's HR Records from the creation of the record until the record is archived or destroyed, per NERC's regulated records management requirements.
Records Management Process	A process is comprised of identifying records, classifying records, and storing records, as well as coordinating employee and non-employee access.
Regional Entity	In 2007, FERC approved agreements by which NERC delegates its authority to monitor and enforce compliance to six Regional Entities. The members of the Regional Entities come from all segments of the electricity industry: investor-owned utilities; federal power agencies; rural electric cooperatives; state, municipal, and provincial utilities; independent power producers; power marketers; and end-use customers. These entities account for virtually all the electricity supplied in the United States, Canada, and the northern portion of Baja California, Mexico. See MRO, NPCC, RF, SERC, Texas RE, WECC.
Repository	A managed unit of content and metadata storage and includes areas on the file system and a database.
Retainer	A retainer is a set of states that define the stages in a record's life.
RF	ReliabilityFirst (Regional Entity)
SBO	Service Based Object
SEL	Secure Evidence Locker
SERC	SERC Reliability Corporation (Regional Entity)
TBO	Type Based Object
Texas RE	Texas Reliability Entity (Regional Entity)
TLS	Transport Layer Security (e.g. TLS 1.2, 1.3)
UAT	User Acceptance Testing
VDI	Virtual Desktop Infrastructure
WECC	Western Electricity Coordinating Council (Regional Entity)

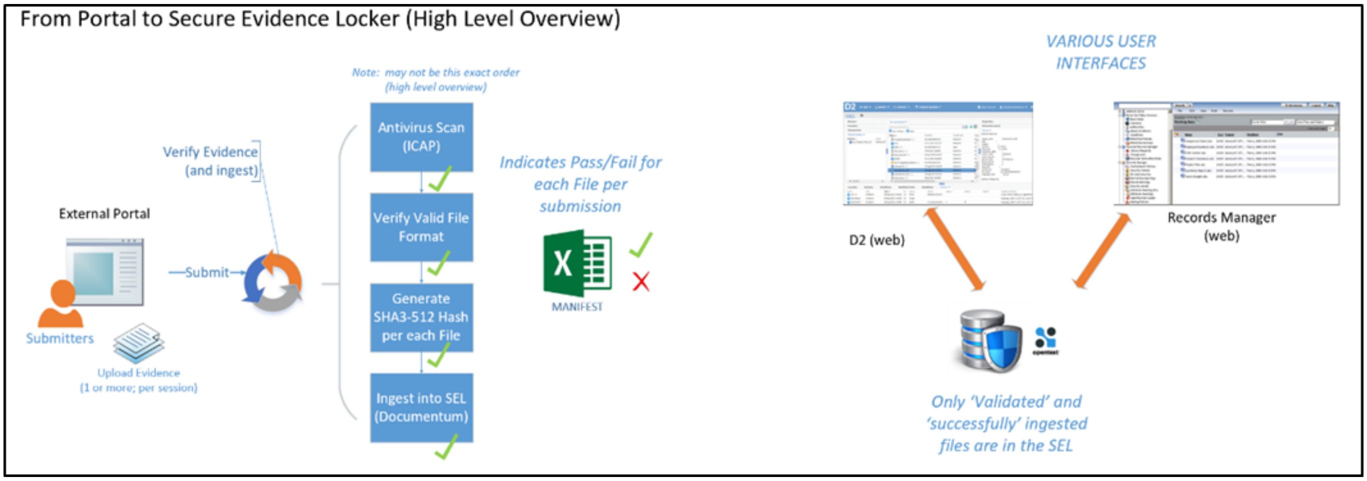
NERC SEL Overview

The NERC SEL Documentum D2 implementation is a highly-secure repository for documents submitted through the NERC SEL portal. Portal users submit documents which are encrypted and stored in the appropriate location (Region/Entity/Activity), and accessible only to NERC SEL users with the proper permissions and access.

The NERC SEL Workflow

The image below shows the high-level process for the NERC SEL platform.

NOTE: Only Administrators will have access to the Records Manager interface.



The Align system provides the validation code (Align reference) to the person who will be submitting evidence. This user, the submitter, will enter the value into the NERC SEL portal, along with documents.

The Align reference value will have information needed to locate the proper location in the SEL to store the submitted content. If the submitter is adding to an existing activity, the content is added to the existing activity. If the activity is new, the NERC SEL system will create the activity and the necessary subfolders (Evidence, Work, Records). A new activity will not have a custodian or analysts until they are assigned.

After successfully uploading his/her evidence through the portal, the submitter receives a notification confirming their submission.

The Entity Relationship Manager in the NERC SEL system receives a notification that new content has been submitted. The CEA custodian can then assign custodians and analysts to work on the activity.

Access

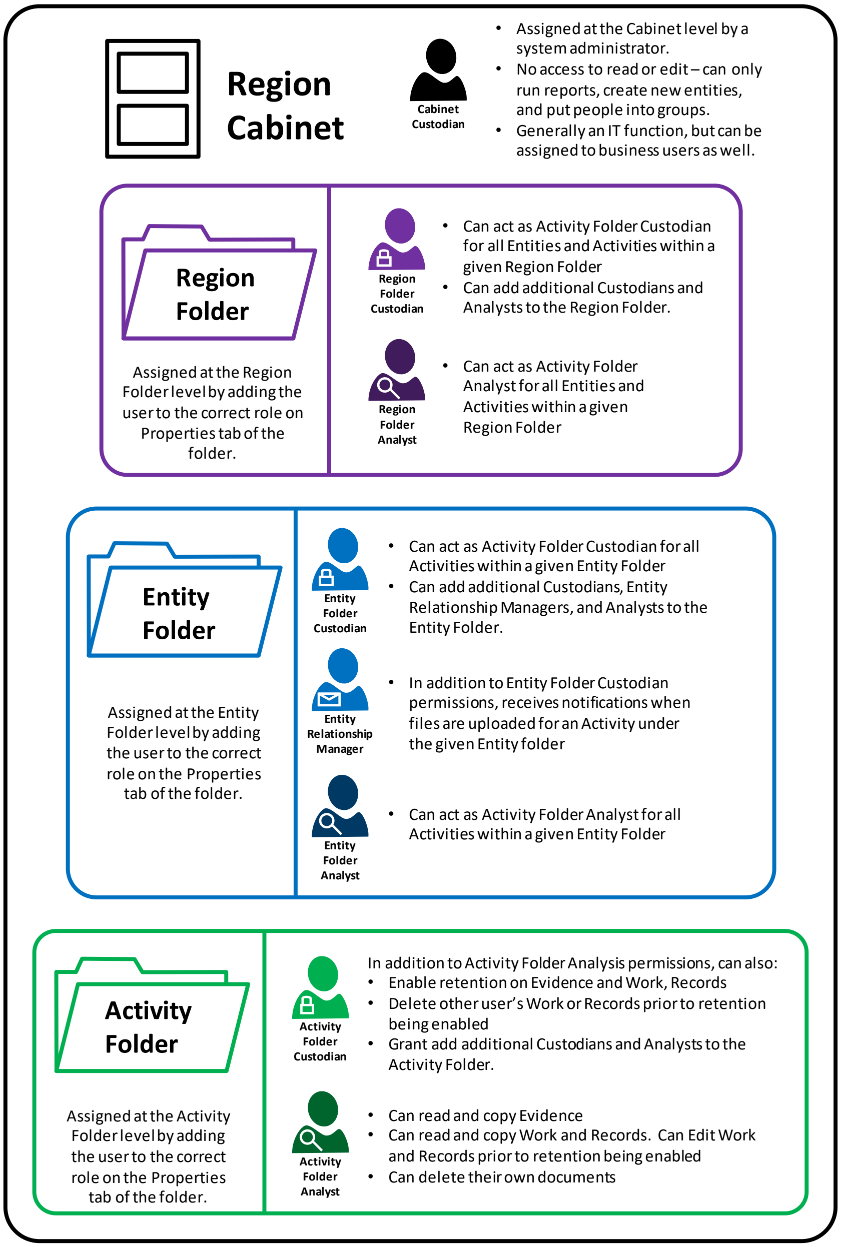
NERC SEL Documentum users are assigned specific access to entities. Users can manage documents within those entities only. There are several tiers of access, and several types of access (roles). Users can be given different types of access in different tiers.

Tiers

- Region, for example, MRO
- Entity, for example, NCR00102
- Activity, for example, VI2020-00001

Roles

Roles are summarized in the diagram below:



- Assigned at the Cabinet level by a system administrator.
- No access to read or edit – can only run reports, create new entities, and put people into groups.
- Generally an IT function, but can be assigned to business users as well.

Assigned at the Region Folder level by adding the user to the correct role on Properties tab of the folder.

- Can act as Activity Folder Custodian for all Entities and Activities within a given Region Folder
- Can add additional Custodians and Analysts to the Region Folder.

- Can act as Activity Folder Analyst for all Entities and Activities within a given Region Folder

Assigned at the Entity Folder level by adding the user to the correct role on the Properties tab of the folder.

- Can act as Activity Folder Custodian for all Activities within a given Entity Folder
- Can add additional Custodians, Entity Relationship Managers, and Analysts to the Entity Folder.

- In addition to Entity Folder Custodian permissions, receives notifications when files are uploaded for an Activity under the given Entity folder

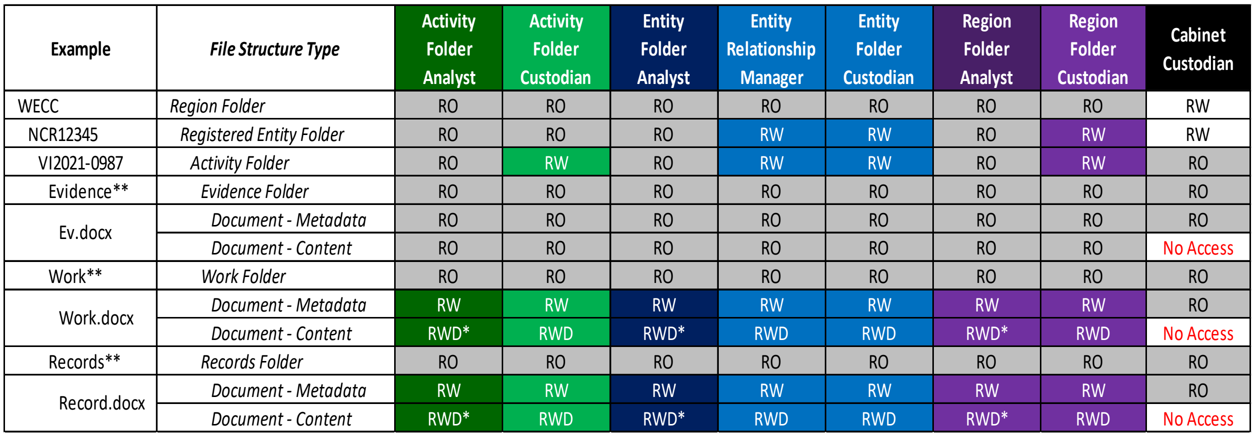
- Can act as Activity Folder Analyst for all Activities within a given Entity Folder

Assigned at the Activity Folder level by adding the user to the correct role on the Properties tab of the folder.

In addition to Activity Folder Analysis permissions, can also:
- Enable retention on Evidence and Work, Records
- Delete other user's Work or Records prior to retention being enabled
- Grant add additional Custodians and Analysts to the Activity Folder.

- Can read and copy Evidence
- Can read and copy Work and Records. Can Edit Work and Records prior to retention being enabled
- Can delete their own documents

User roles and the content they can access and edit is shown in the table below.



Example	*File Structure Type*	Activity Folder Analyst	Activity Folder Custodian	Entity Folder Analyst	Entity Relationship Manager	Entity Folder Custodian	Region Folder Analyst	Region Folder Custodian	Cabinet Custodian
WECC	*Region Folder*	RO	RO	RO	RO	RO	RO	RO	RW
NCR12345	*Registered Entity Folder*	RO	RO	RO	RW	RW	RO	RW	RW
VI2021-0987	*Activity Folder*	RO	RW	RO	RW	RW	RO	RW	RO
Evidence**	*Evidence Folder*	RO	RO	RO	RO	RO	RO	RO	RO
Ev.docx	*Document - Metadata*	RO	RO	RO	RO	RO	RO	RO	RO
	Document - Content	RO	RO	RO	RO	RO	RO	RO	No Access
Work**	*Work Folder*	RO	RO	RO	RO	RO	RO	RO	RO
Work.docx	*Document - Metadata*	RW	RW	RW	RW	RW	RW	RW	RO
	Document - Content	RWD*	RWD	RWD*	RWD	RWD	RWD*	RWD	No Access
Records**	*Records Folder*	RO	RO	RO	RO	RO	RO	RO	RO
Record.docx	*Document - Metadata*	RW	RW	RW	RW	RW	RW	RW	RO
	Document - Content	RWD*	RWD	RWD*	RWD	RWD	RWD*	RWD	No Access

RO = Read Only   RW = Read Write   RWD = Read Write Delete

***** Can only delete the content they create

****** Once a retention policy has been applied to content in this folder, it cannot be deleted.

Activities

When a submitter adds content through the portal, they provide the reference ID number that sends the content to the correct activity.

If the submitter is adding documents for a new activity, the activity will be created automatically when they submit the content through the portal.

Records Management

The NERC SEL Documentum D2 system is a content management system that includes records management functionality. The Records Manager user can apply a retention schedule to content that has been completed in the system. The retention policy defines how long a record is retained.

Records Management Access

For each activity, the activity custodians and the CEA custodian can modify the records management for the given activity. See Apply Retention below for more details.

A small group of records managers and system administrators will have access to the records management user interface. The RM user interface is outside the scope of this guide.

Content Related to a Non-Compliance and Not Related to Non-Compliance

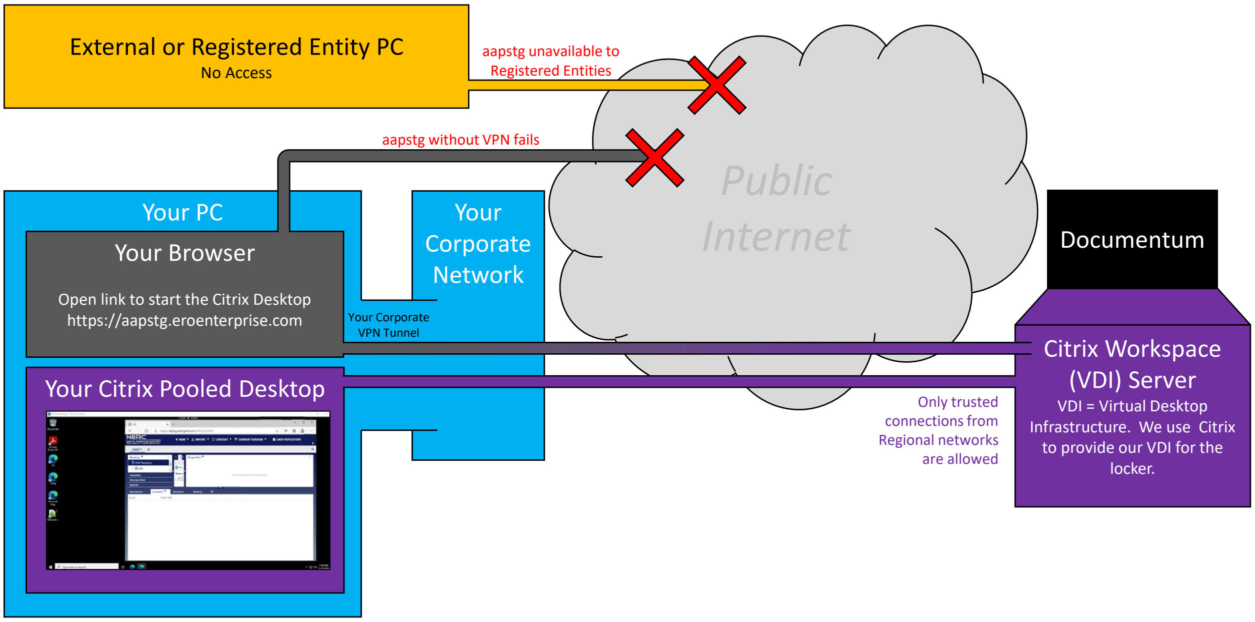
After an activity is closed and the final determination is made, the custodian can apply retention to the records which will determine when the content will be destroyed.

Related to a Non-Compliance – when an activity is closed and the final determination is made, the custodian edits the properties to select the Records Start Date to start the retention policy.

Not Related to Non-Compliance – when the activity is closed and the content that is not related to non-compliance, the custodian can apply retention to Evidence & Work, which will destroy that content in 90 days. Users can select content and view the records management properties.

Login

Connections to the SEL are only allowed through NERC or Regional corporate networks - other connection requests are denied. If you are on your VPN and you are unable to connect to the SEL (i.e., you get an error that says the system is unreachable or unavailable), then it is likely that your connection request is not being routed through your corporate network. Show this diagram to your support team and ask for their assistance.


External or Registered Entity PC
No Access
aapstg unavailable to Registered Entities
aapstg without VPN fails
Public Internet
Your PC
Your Browser
Open link to start the Citrix Desktop
https://aapstg.eroenterprise.com
Your Corporate Network
Your Corporate VPN Tunnel
Documentum
Citrix Workspace (VDI) Server
VDI = Virtual Desktop Infrastructure. We use Citrix to provide our VDI for the locker.
Your Citrix Pooled Desktop
Only trusted connections from Regional networks are allowed

You must have the Citrix Workspace application installed. If you try to go to the link listed below and get an error that asks if want to download a file, or choose an app to open a file, then you probably do not have the Citrix Workspace application installed. Ask your support team to help you get this application installed.

You will not be able to each the Documentum system directly from your PC. You can ONLY access the Documentum system from inside your Citrix Pooled Desktop session.

Logging into the SEL Analysis Environment as a Regional User
The SEL is a highly secured environment. To access it, you will need to do a number of things.

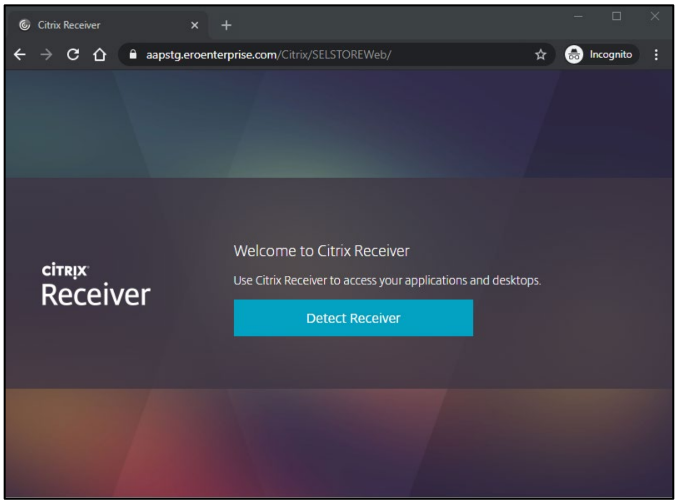
1.) You, or your IT Staff, will need to download and install the Citrix Workspace application. The installation requires administrator privileges and a system reboot.
2.) Use your web browser to go to:

https://aap.eroenterprise.com

3.) Log in with your ERO Portal account

Login

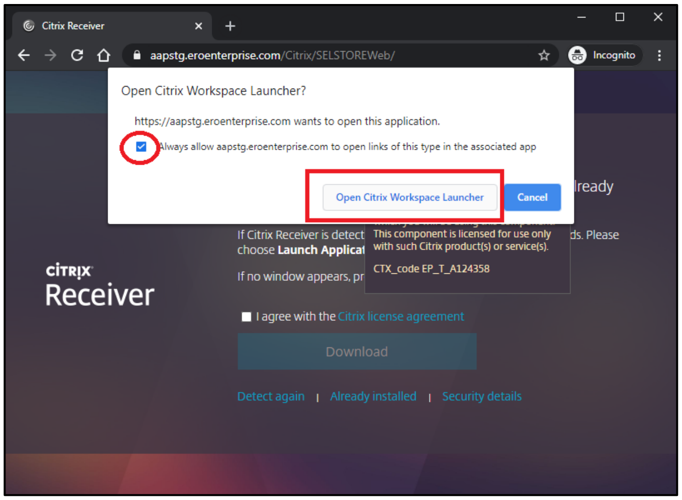
4.) The first time you log in, you may see the Citrix Receiver screen. Click "Detect Receiver."



Welcome to Citrix Receiver

Use Citrix Receiver to access your applications and desktops.

1.) You will then be prompted to open the Citrix Workspace Launcher. Check the box and click "Open Citrix Workspace Launcher."



Citrix Receiver
aapstg.eroenterprise.com/Citrix/SELSTOREWeb/
Incognito
CITRIX
Receiver

Open Citrix Workspace Launcher?

https://aapstg.eroenterprise.com wants to open this application.

☑ Always allow aapstg.eroenterprise.com to open links of this type in the associated app

Open Citrix Workspace Launcher
Cancel
lready

If Citrix Receiver is detect ds. Please choose **Launch Applicat**

If no window appears, pr

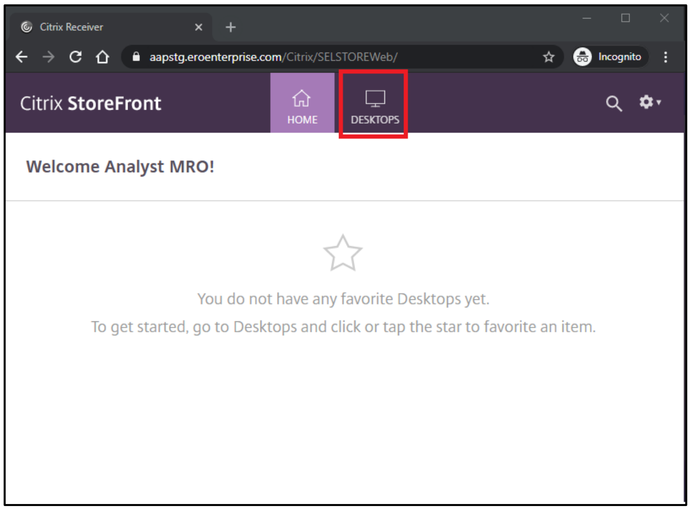
This component is licensed for use only with such Citrix product(s) or service(s).

CTX_code EP_T_A124358

□ I agree with the Citrix license agreement

Login

Next, you will be presented with the Citrix StoreFront. Choose “Desktops.”

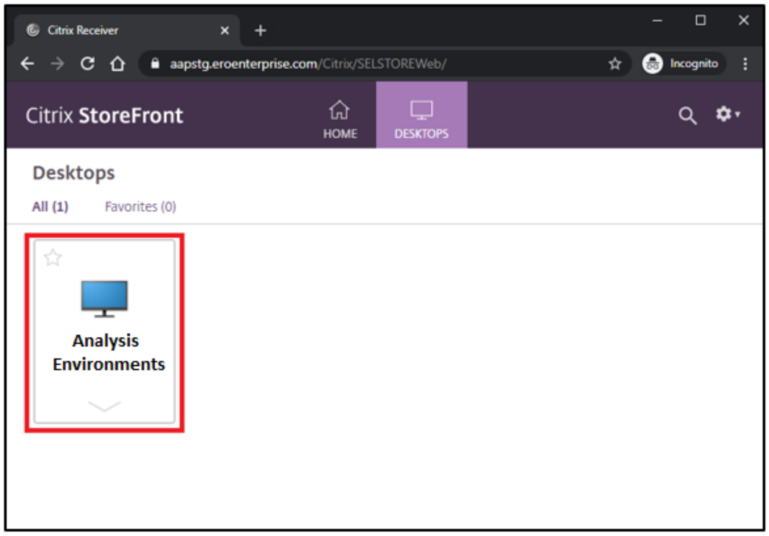


Welcome Analyst MRO!

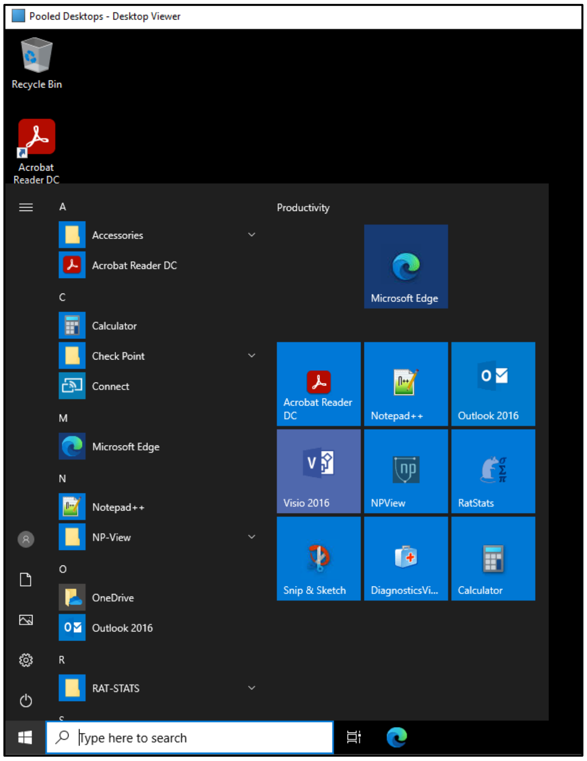
You do not have any favorite Desktops yet.

To get started, go to Desktops and click or tap the star to favorite an item.

Then choose “Analysis Environments.”



Login

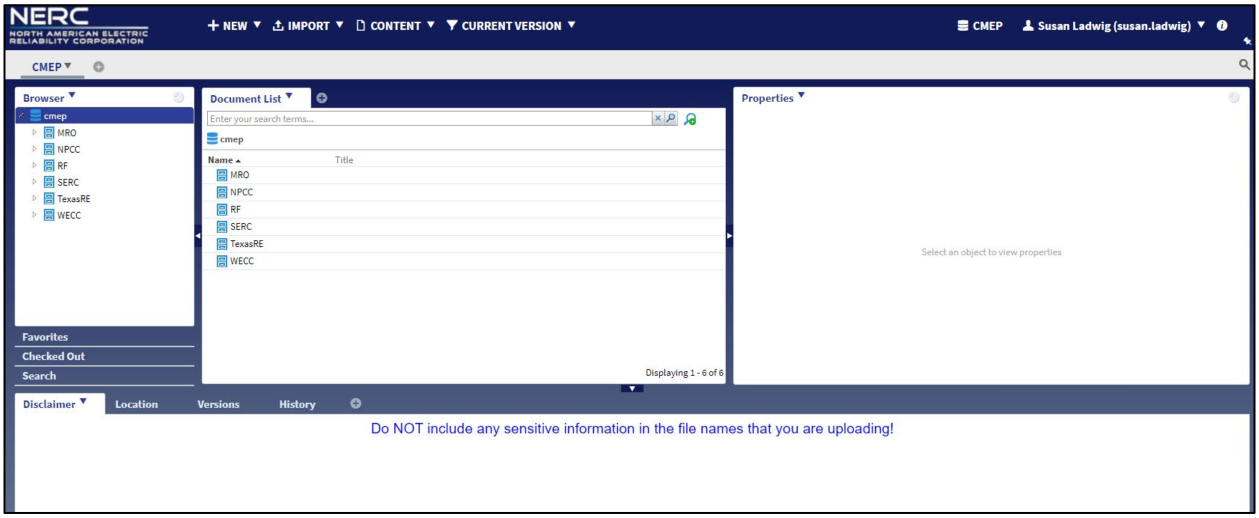


At this point, your Analysis Environment will be instantiated, and you should be able to begin working. Go to the Start menu to access your applications.

Documentum D2 is a web-based application. Open the link to D2 from the desktop icon. You will automatically be logged in to D2.

Using Documentum D2

After signing in to the system you will land on your D2 dashboard.



Do NOT include any sensitive information in the file names that you are uploading!

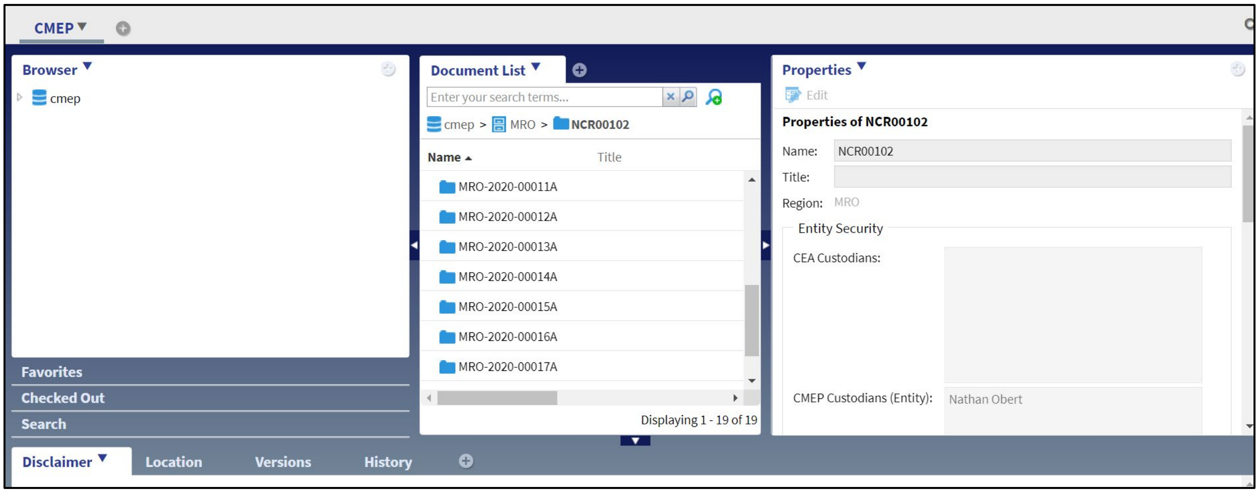
Your D2 Dashboard

The D2 dashboard layout includes:

- Browser – browse folders and files
- Document List – displays documents in the selected folder
- Properties – displays properties of the selected entity (entity, folder, document)
- Favorites – view a list of content that you have set as favorite
- Checked Out – view a list of content that you have checked out
- Search – locate files using search criteria

D2 Page Layout

The default NERC SEL Documentum D2 page layout has three columns.



Properties of NCR00102

Name: NCR00102

Title:

Region: MRO

Entity Security

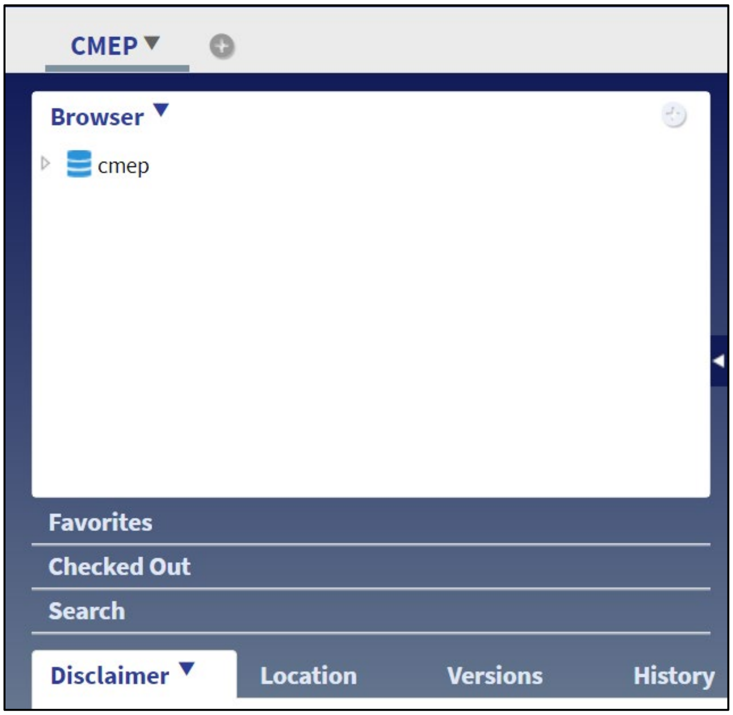
CEA Custodians:

CMEP Custodians (Entity): Nathan Obert

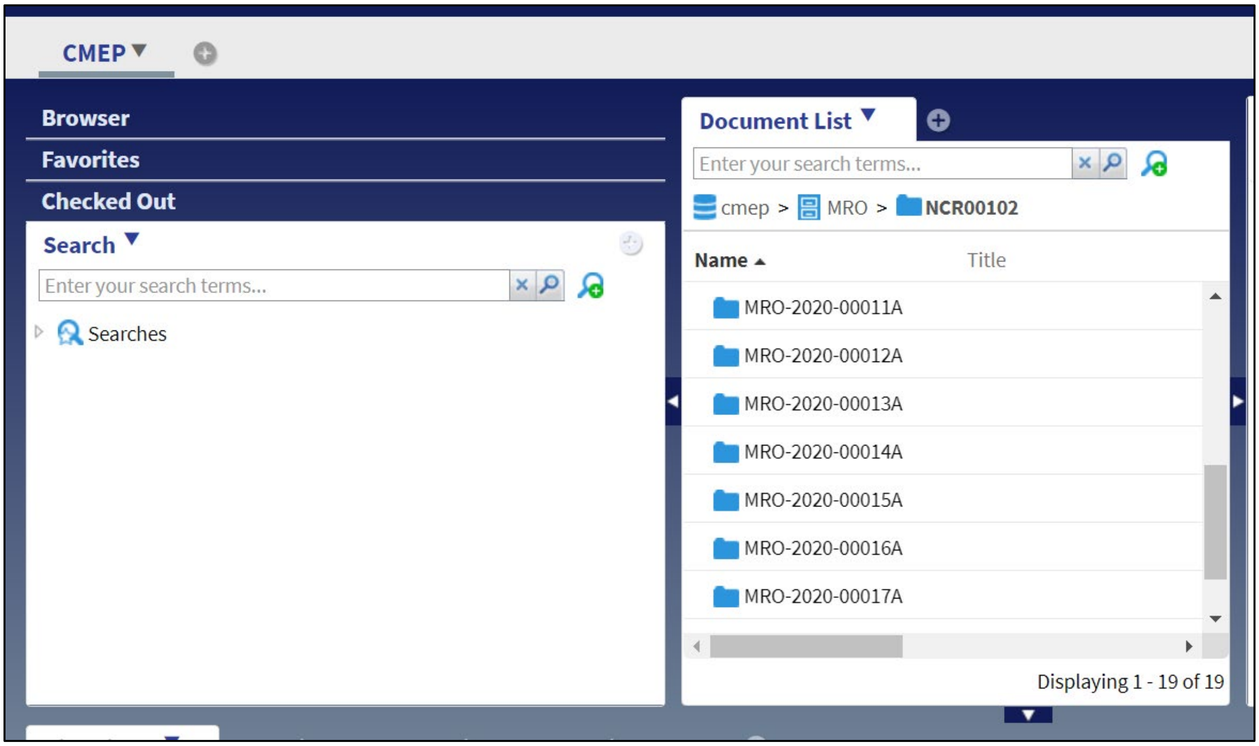
The left column lists the main functional areas:

- Browser
- Favorites
- Checked Out
- Search.

⚠ **NOTE** the disclaimer that reminds users not to include any sensitive information in file names.

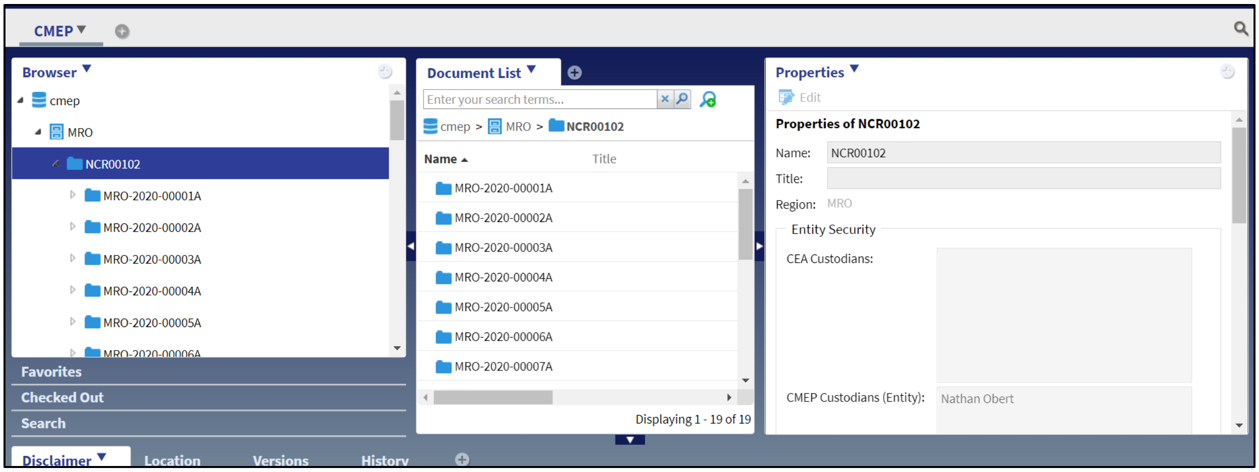


The center column displays the contents of the selected container you have opened using Browser. The display does not change if you select another function, for example, Search.



Name	Title
MRO-2020-00011A	
MRO-2020-00012A	
MRO-2020-00013A	
MRO-2020-00014A	
MRO-2020-00015A	
MRO-2020-00016A	
MRO-2020-00017A	

The right-hand column displays the Properties of the selected entity or document.



Name	Title
MRO-2020-00001A	
MRO-2020-00002A	
MRO-2020-00003A	
MRO-2020-00004A	
MRO-2020-00005A	
MRO-2020-00006A	
MRO-2020-00007A	

Properties of NCR00102

Name: NCR00102

Title:

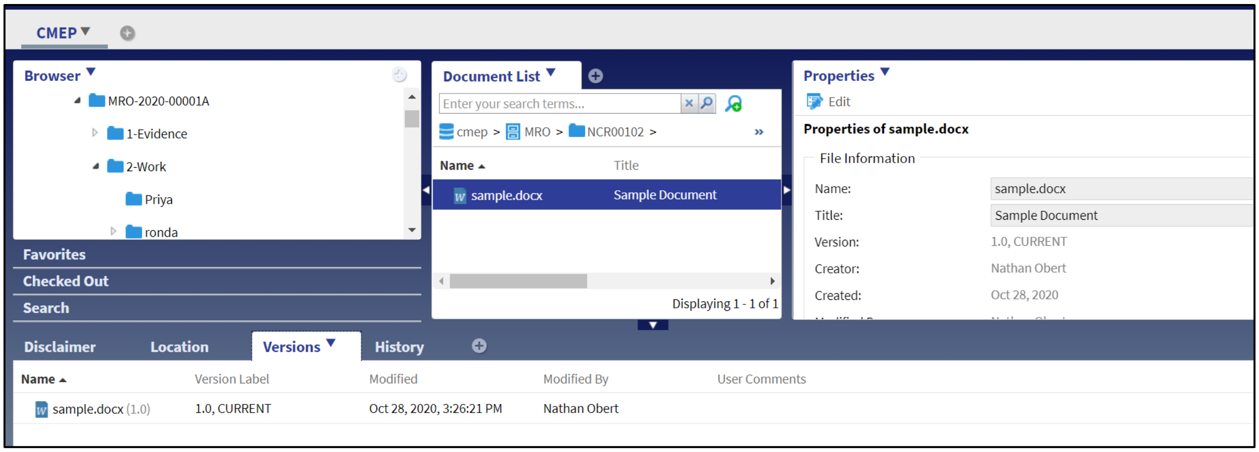
Region: MRO

CEA Custodians:

CMEP Custodians (Entity): Nathan Obert

You can view the properties of content you have access to by navigating to the region/entity/activity/file.

At the bottom of the screen there are tabs for Location, Versions, and History. These tabs display information for the selected document. Navigate to a document, then click through the tabs to view its location, versions, and history.



Name	Title
sample.docx	Sample Document

Displaying 1 - 1 of 1

Properties of sample.docx

File Information

Name:	sample.docx
Title:	Sample Document
Version:	1.0, CURRENT
Creator:	Nathan Obert
Created:	Oct 28, 2020

Name	Version Label	Modified	Modified By	User Comments
sample.docx (1.0)	1.0, CURRENT	Oct 28, 2020, 3:26:21 PM	Nathan Obert	

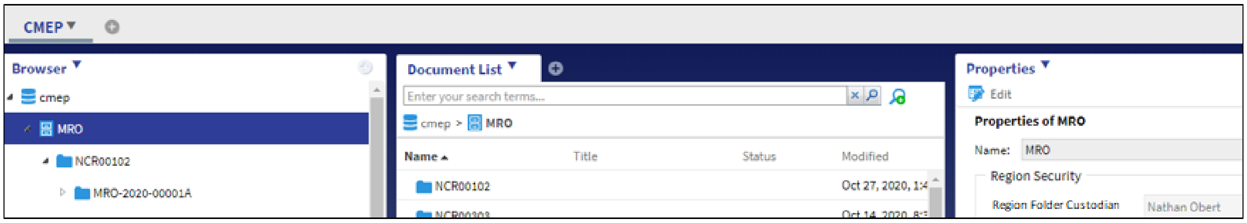
Assign/Remove Access

Access to content is controlled by the custodian at that level. The Cabinet Custodian controls region folder access, the Region Folder Custodian controls entity folder access, and the Entity Folder Custodian controls activity folder access. Adding and removing access is described below.

Cabinet Custodian Assign Access to Region

The cabinet custodian can assign users as Region Folder Custodians and Region Folder Analysts. To assign a user to Regional Folder Custodian or Analyst role:

1. Select the **Browser** function if necessary.
2. Select the Region, for example, MRO.
3. On the Properties panel at the right, click Edit.



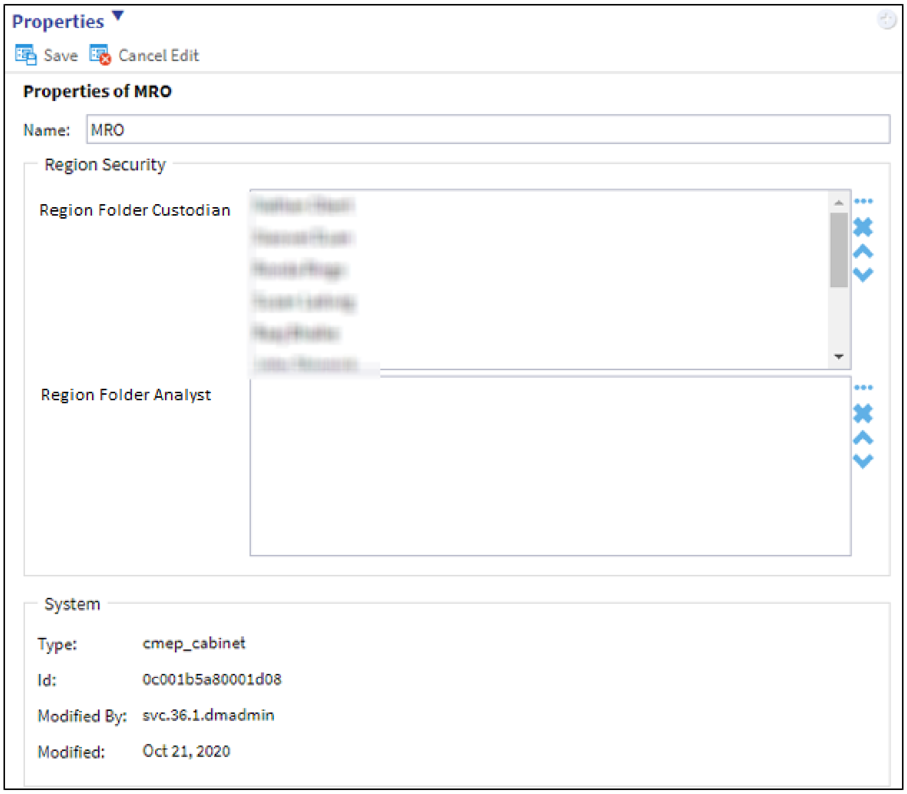
Properties of MRO

Name: MRO

Region Security

Region Folder Custodian: Nathan Obert

The properties panel opens for editing.



Properties of MRO

Name: MRO

Region Security

Region Folder Custodian

Region Folder Analyst

System

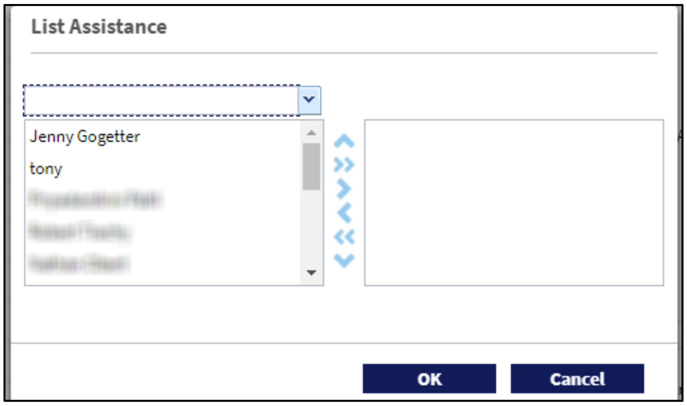
Type: cmep_cabinet

Id: 0c001b5a80001d08

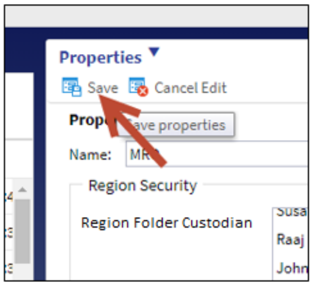
Modified By: svc.36.1.dmadmin

Modified: Oct 21, 2020

4. Click the ellipsis (…) at the top of the field to which you wish to add a user (Region Folder Custodians or Region Folder Analysts. The user picker opens.



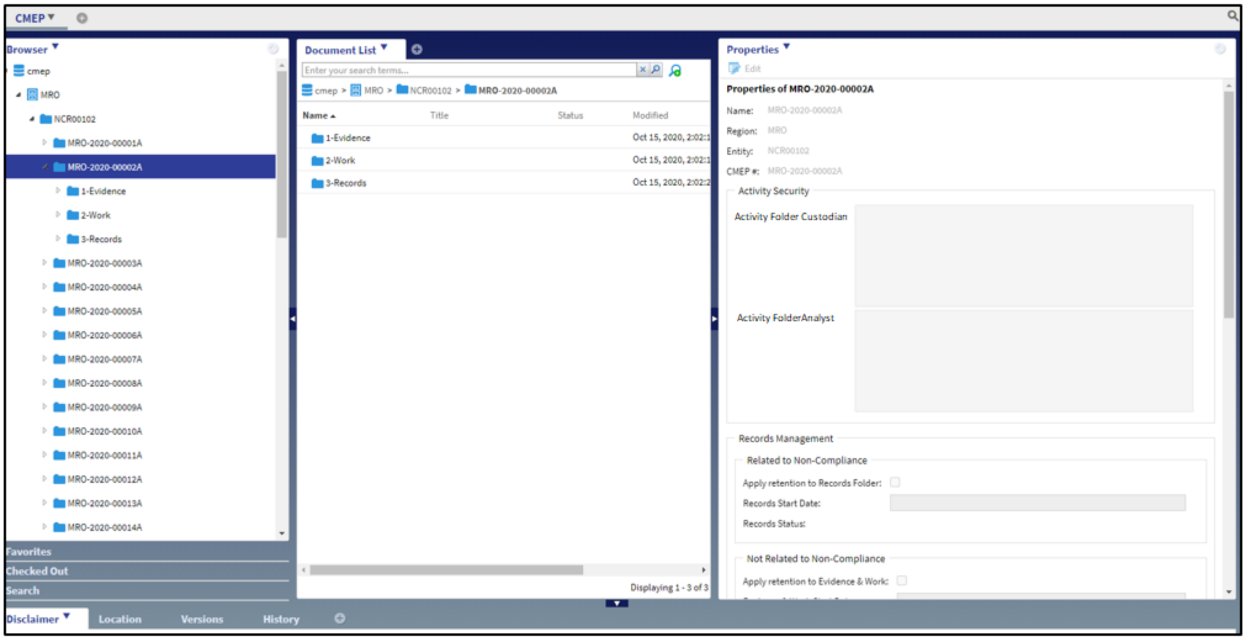
5. Select the name of the user to be added to the list and click the right arrow to move the user to the role. Repeat for any additional users to be provided the role.
6. Click **OK**
7. Click **Save** on the Properties panel.



Entity Relationship Manager Assign Access to Activity

When the Entity Relationship Manager receives notification that new content has been submitted, he/she must assign access to the new content.

1. Locate the new activity in NERC SEL. You can navigate to the activity, or use search. See the Search section for tips on locating content. You can copy the text from the email notification and use it in the search field.



cmep
MRO
NCR00102
MRO-2020-00001A
MRO-2020-00002A
1-Evidence
2-Work
3-Records
MRO-2020-00003A
MRO-2020-00004A
MRO-2020-00005A
MRO-2020-00006A
MRO-2020-00007A
MRO-2020-00008A
MRO-2020-00009A
MRO-2020-00010A
MRO-2020-00011A
MRO-2020-00012A
MRO-2020-00013A
MRO-2020-00014A

Enter your search terms...

cmep > MRO > NCR00102 > MRO-2020-00002A

Name ▲	Title	Status	Modified
1-Evidence			Oct 15, 2020, 2:02:1
2-Work			Oct 15, 2020, 2:02:1
3-Records			Oct 15, 2020, 2:02:2

Displaying 1 - 3 of 3

Properties of MRO-2020-00002A

Name: MRO-2020-00002A
Region: MRO
Entity: NCR00102
CMEP #: MRO-2020-00002A

Activity Security

Activity Folder Custodian

Activity FolderAnalyst

Records Management

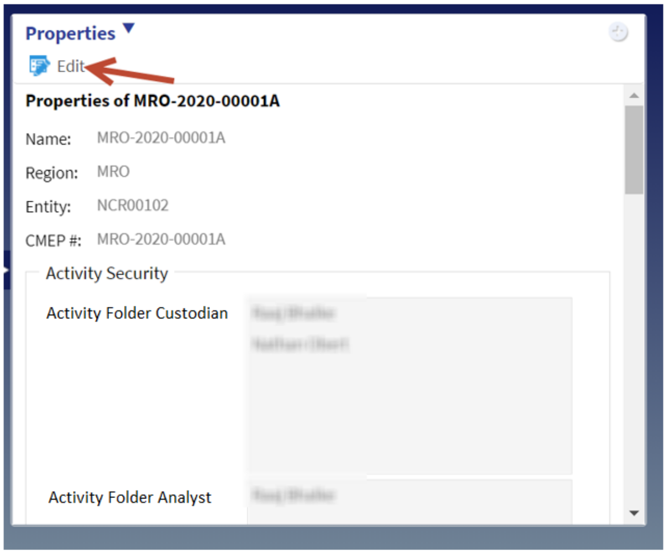
Related to Non-Compliance

Apply retention to Records Folder: □
Records Start Date:
Records Status:

Not Related to Non-Compliance

Apply retention to Evidence & Work: □

2. Select the activity, for example, MRO-2020-00001A.
3. On the Properties panel at the right, click **Edit**.



Properties of MRO-2020-00001A

Name: MRO-2020-00001A
Region: MRO
Entity: NCR00102
CMEP #: MRO-2020-00001A

Activity Security

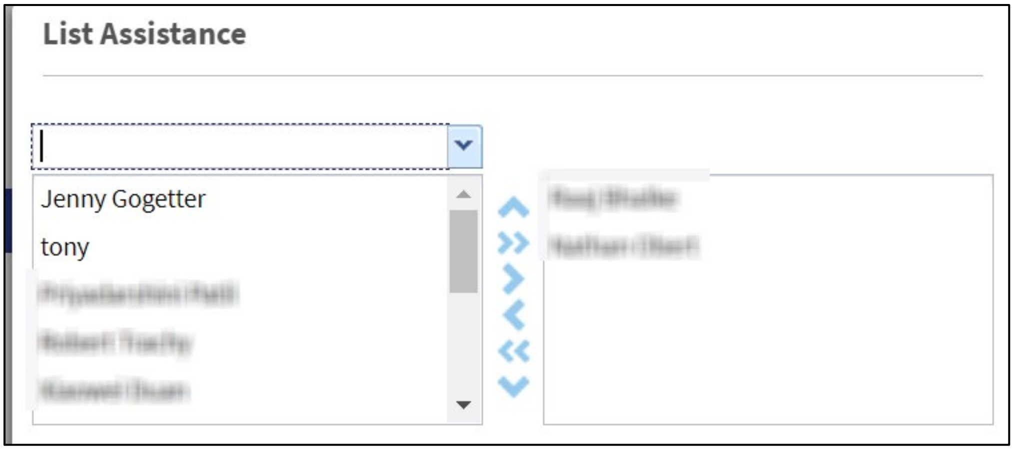
Activity Folder Custodian [redacted] [redacted]

Activity Folder Analyst [redacted]

The properties opens for editing.

4. Scroll to the Activity Security section.
5. Click the ellipsis (…) at the right of the custodian or analyst field to add a user.

The user pick list opens.



6. Select the name of the user to be added to the list and click the right arrow to move the user to the role. Repeat for any additional users to be provided the role.
7. Click **OK**
8. Click **Save** on the Properties panel.

Remove Access

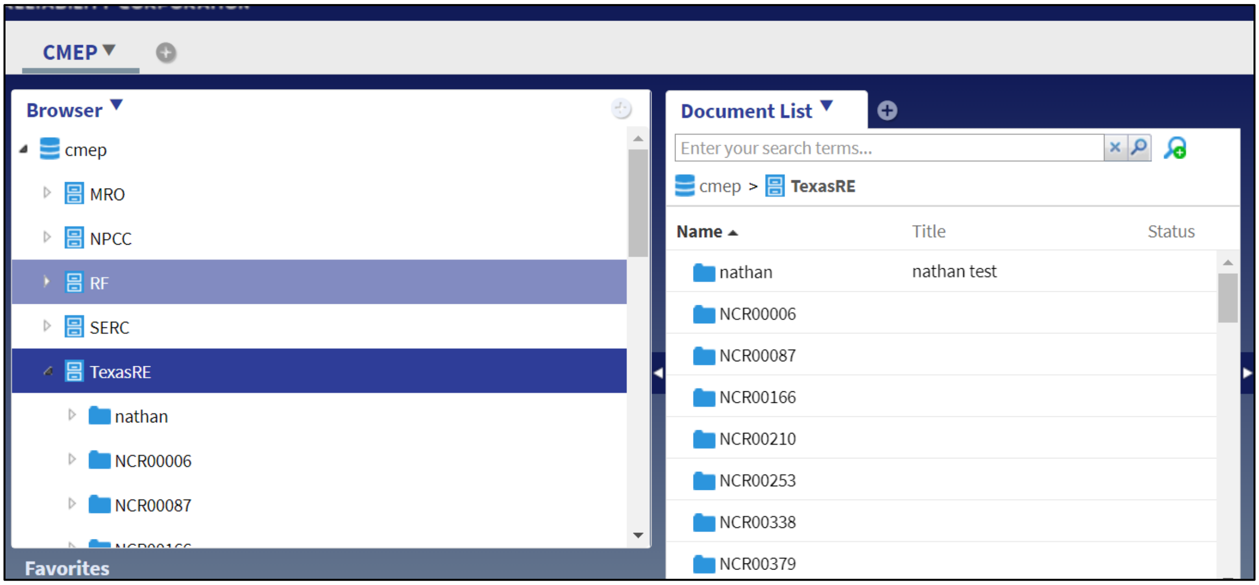
The Cabinet Custodian and Regional Folder Custodian can also remove user's access to content.

The process to remove a user from a role is similar to the assignment. Move the user name from the right-hand column to the left using the left arrow. Remember to save the properties when done.

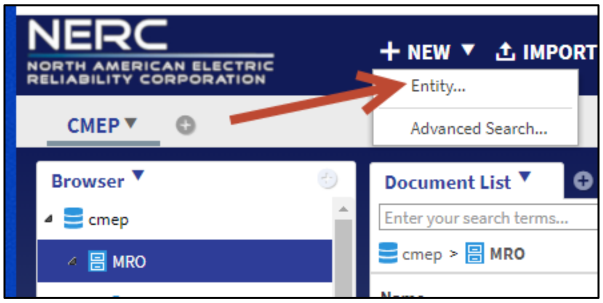
Create Registered Entity Container

The Cabinet Custodian can create a new Registered Entity Container.

1. Select Browser if necessary.
2. Select the registered entity for the new container, for example TexasRE.

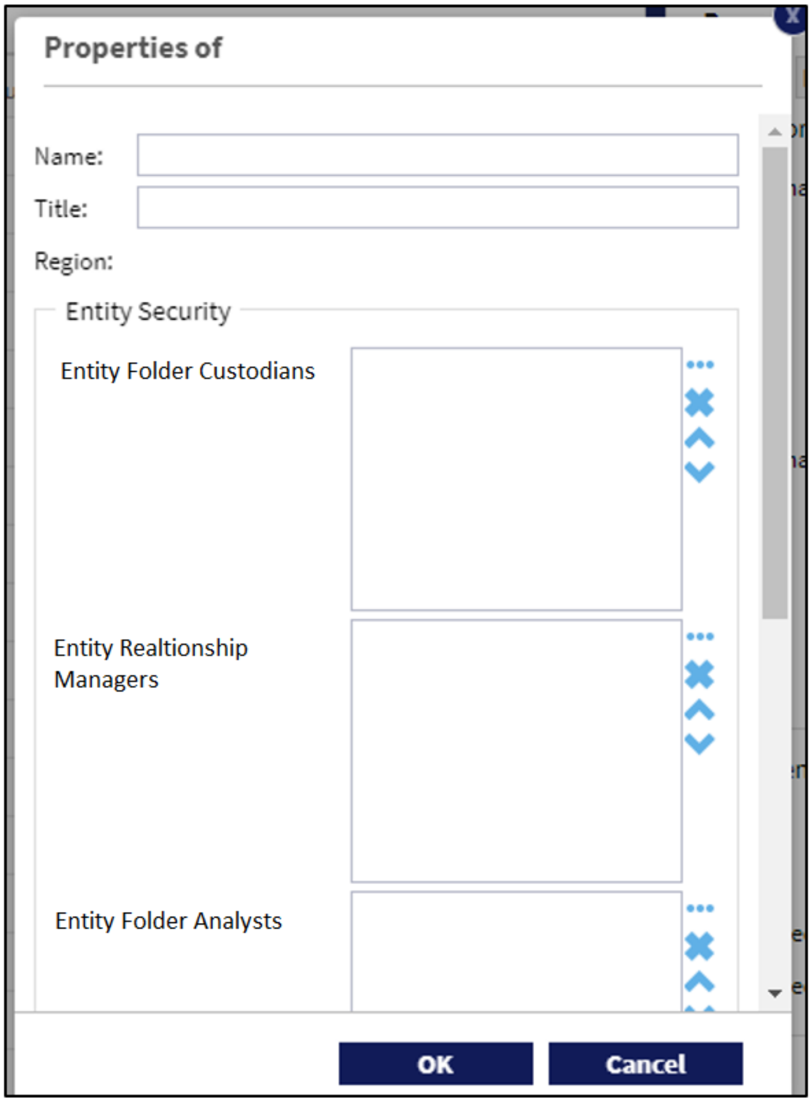


3. Select the Region name and choose New →Entity.



4. Complete the information for the new entity.
5. Click **OK**.

Create Registered Entity Container



Properties of

Name:

Title:

Region:

Entity Security

Entity Folder Custodians

Entity Realtionship Managers

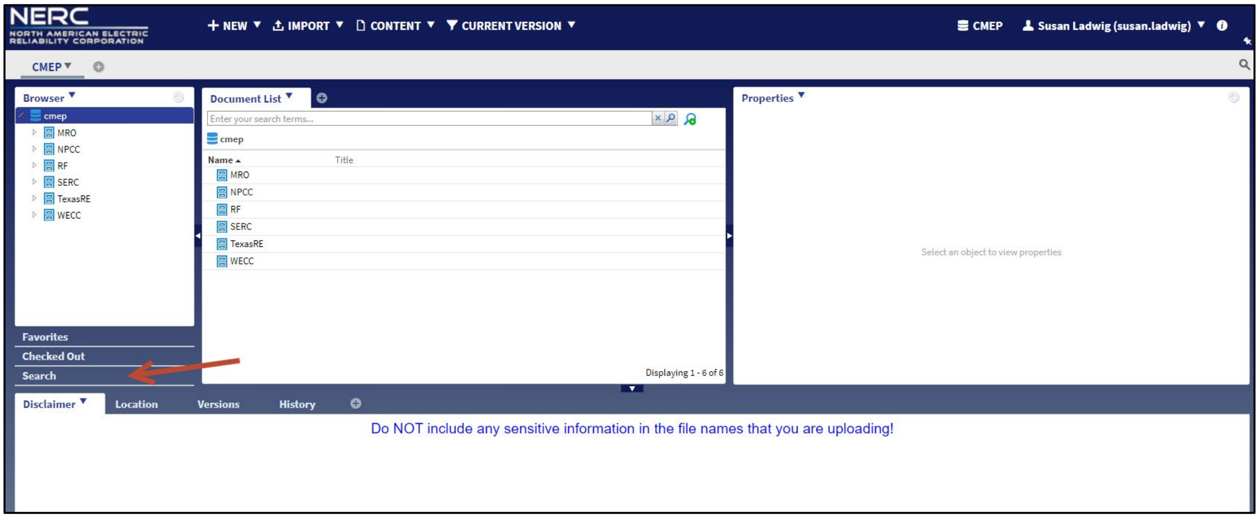
Entity Folder Analysts

Search

The search function in NERC SEL will help you locate content quickly. You can use a basic search or an advanced search. Remember you can also use the saved search described above to locate your activities.

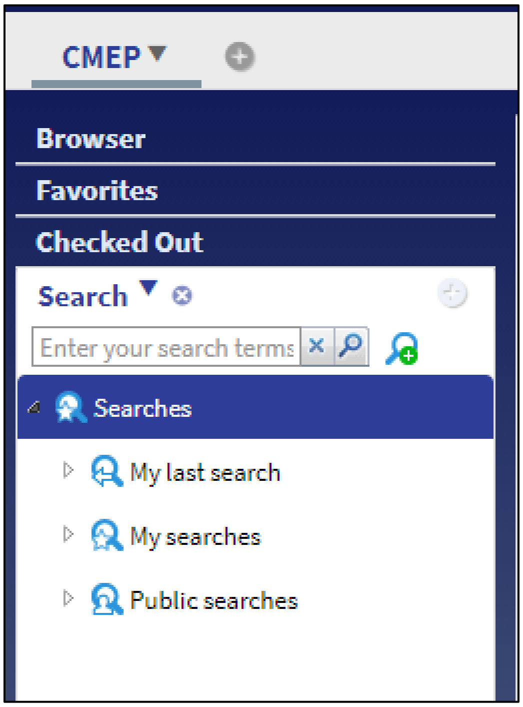
Basic Search

1. Select the Search function on the left-hand menu.

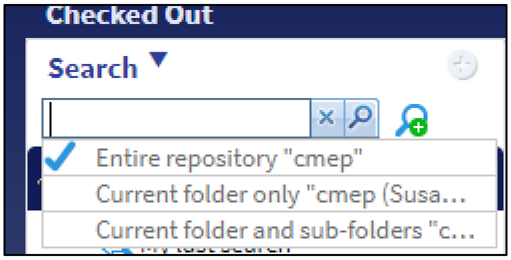


Do NOT include any sensitive information in the file names that you are uploading!

The NERC SEL D2 search menu opens.



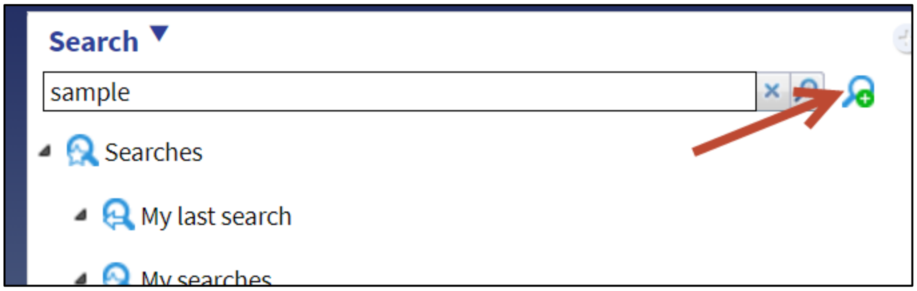
2. Enter a search term, or select from the menu items for a saved search. You can choose to search the entire repository, current folder, or current folder and subfolders.
3. Click the search icon. A list of matches is returned.


Checked Out
Search
Entire repository "cmep"
Current folder only "cmep (Susa...
Current folder and sub-folders "c...

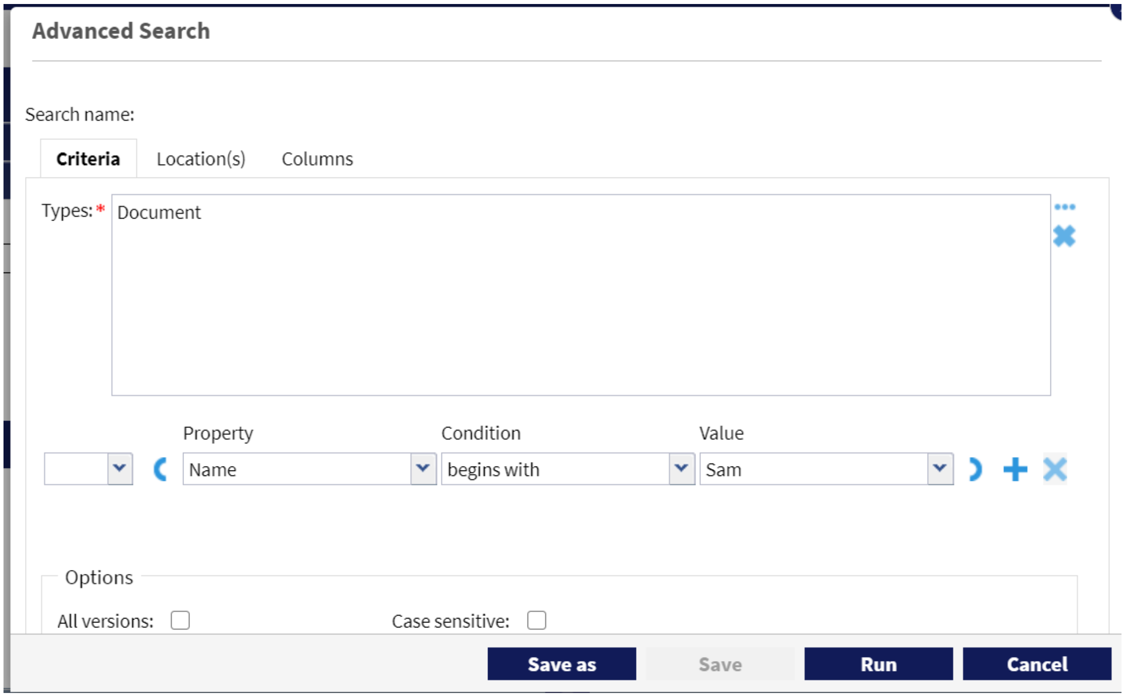
Advanced Search

You can use Advanced Search to use properties to filter down search results. You can also use Criteria, Location(s), or Columns in your search.

1. Select Search on the left-hand menu.
2. Click the Advanced Search icon.



3. Specify Criteria:
   a. Select a property and condition. Enter a value. You can also build complex searches by choosing the first drop-down menu to choose **and** or **or** searches.



Advanced Search

Search name:

Types:* Document

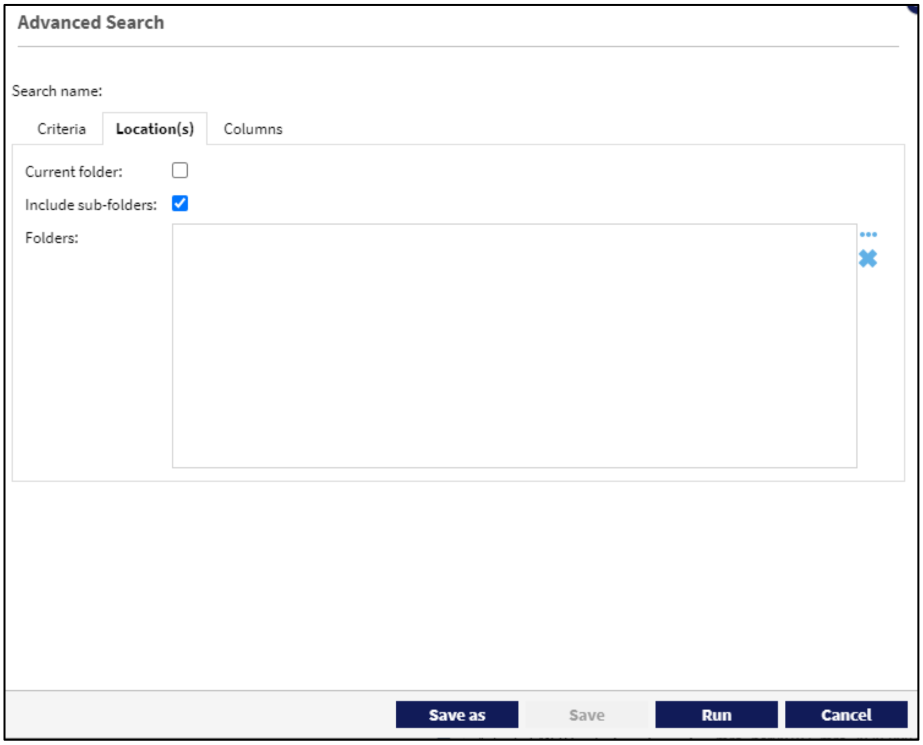
Property	Condition	Value
Name	begins with	Sam

Options

All versions: ☐ Case sensitive: ☐

   b. Click **Run**.

4. Specify Locations:
   a. Select the Location(s) tab.
   b. Select the folders you wish to search. You can select the ellipsis (…) icon and choose the folder from the region/entity/activity structure.
   c. Click Run.



Advanced Search

Search name:

Current folder: ☐

Include sub-folders: ☑

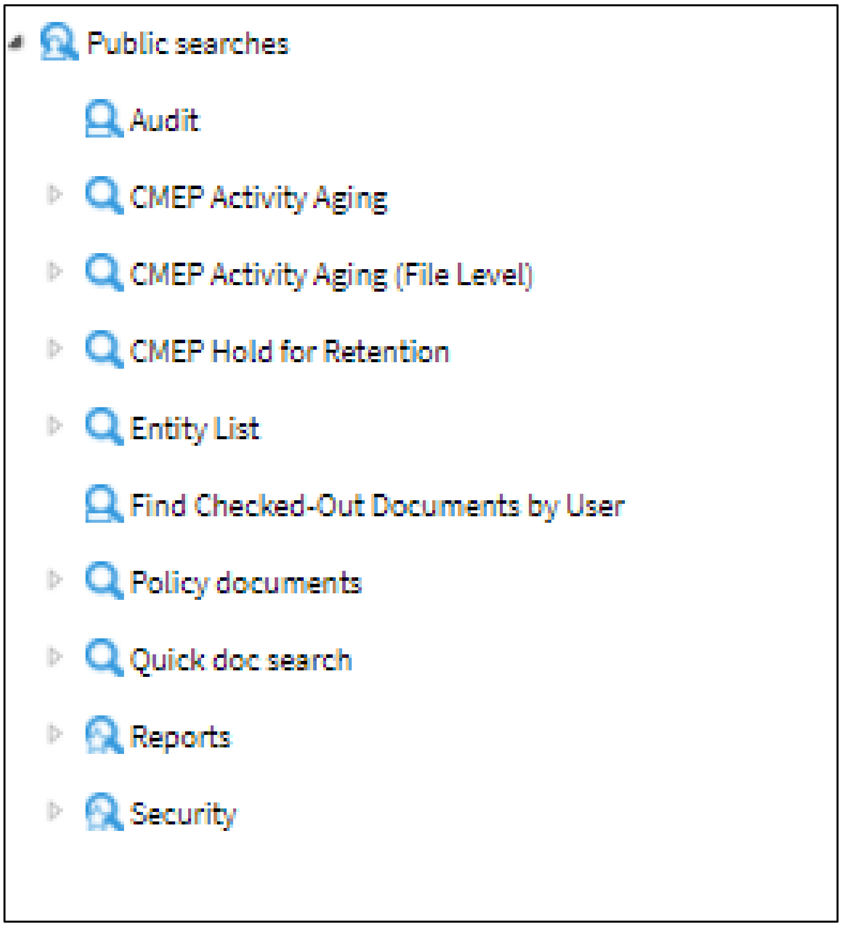
Folders:

5. Specify Columns to include in the results:
    a. Select the Columns tab.
    b. Select the columns for the search result. You can select a column to sort by, and choose to sort by ascending or Descending.
    c. Click Run.

NOTE: You can also choose to save a search by selecting **Save as**.

Public Searches

The system has a number of configured, saved searches in the Public Searches folder.



- Public searches
    - Audit
    - CMEP Activity Aging
    - CMEP Activity Aging (File Level)
    - CMEP Hold for Retention
    - Entity List
    - Find Checked-Out Documents by User
    - Policy documents
    - Quick doc search
    - Reports
    - Security

You can use and view these searches. The Public Searches are a good starting point for you to configure your own custom version of a search, for example, filtering the entity or activity.

Edit a Public Search and then save it in your My Searches folder to locate and run it as needed.

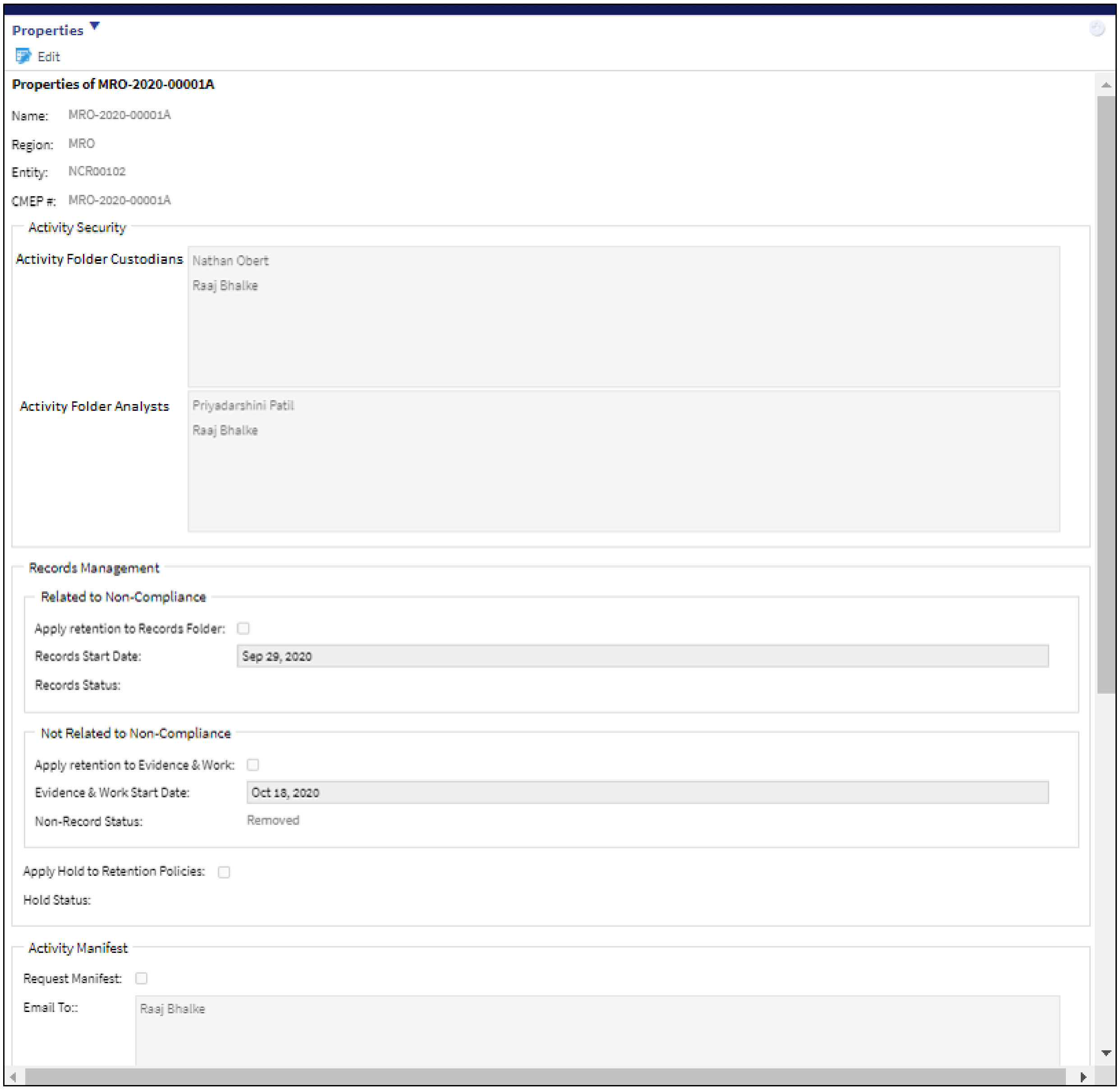
Content Properties

View Properties

To view the properties (metadata) for content:

1. Browse to the content, for example, a cabinet, folder, or subfolder. The Properties panel on the right displays the object's properties.
2. Scroll to view all of the information.

The image below shows the Properties for an activity.



Properties of MRO-2020-00001A

Name: MRO-2020-00001A

Region: MRO

Entity: NCR00102

CMEP #: MRO-2020-00001A

Activity Security

Activity Folder Custodians: Nathan Obert
Raaj Bhalke

Activity Folder Analysts: Priyadarshini Patil
Raaj Bhalke

Records Management

Related to Non-Compliance

Apply retention to Records Folder: □

Records Start Date: Sep 29, 2020

Records Status:

Not Related to Non-Compliance

Apply retention to Evidence & Work: □

Evidence & Work Start Date: Oct 18, 2020

Non-Record Status: Removed

Apply Hold to Retention Policies: □

Hold Status:

Activity Manifest

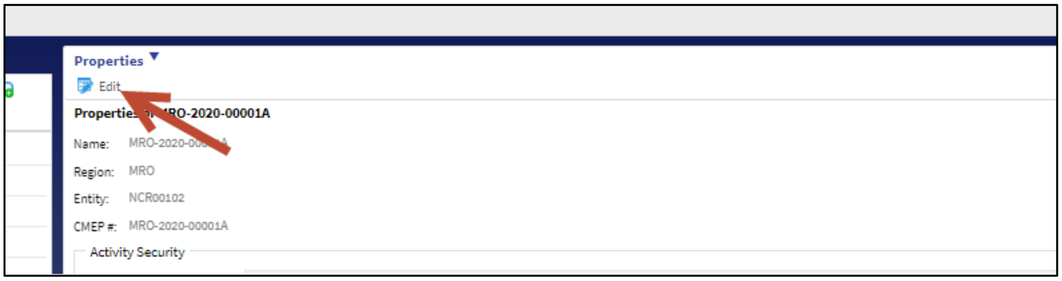
Request Manifest: □

Email To:: Raaj Bhalke

Edit Properties

Users with the proper permissions and access can edit certain values in the properties panel.

1. Browse to the activity to view its properties.
2. On the Properties panel, click Edit.



Properties of MRO-2020-00001A

Name: MRO-2020-00001A

Region: MRO

Entity: NCR00102

CMEP #: MRO-2020-00001A

Activity Security

Here in Edit mode you can:

- Modify the list of users who can access or modify the content. At the activity level, you can add or remove Activity Folder Custodians or Activity Folder Analysts. See Assign/Remove Access section for details.

- Apply retention or apply a hold to content on the properties panel. See Apply Retention to an Activity.

- Request a manifest that is emailed to a specified recipient. See Generate a Manifest.

Document Management

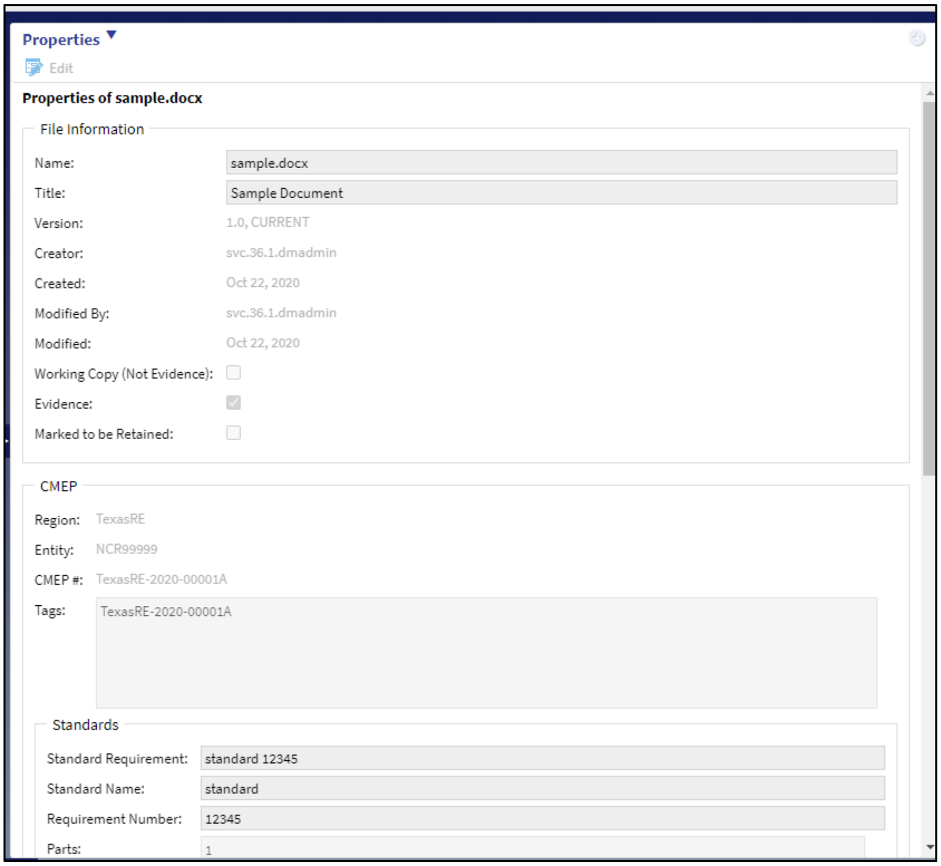
View a Document

1. To view a document, right-click on the file name.
2. Choose View from the drop-down menu.
3. The document will be downloaded to the VDI where you are logged in.
4. Navigate to the document and select it to open it with its native application, for example, Word or Excel.

View Metadata for a Document

When you select a document, the right-hand Properties panel displays the Properties. You can scroll through the panel to view the document's metadata. The metadata is organized in sections:

- File Information
- CMEP (to what entity/region/activity the document belongs)
- Standards



Properties of sample.docx

File Information

Name: sample.docx
Title: Sample Document
Version: 1.0, CURRENT
Creator: svc.36.1.dmadmin
Created: Oct 22, 2020
Modified By: svc.36.1.dmadmin
Modified: Oct 22, 2020
Working Copy (Not Evidence): ☐
Evidence: ☑
Marked to be Retained: ☐

CMEP

Region: TexasRE
Entity: NCR99999
CMEP #: TexasRE-2020-00001A
Tags: TexasRE-2020-00001A

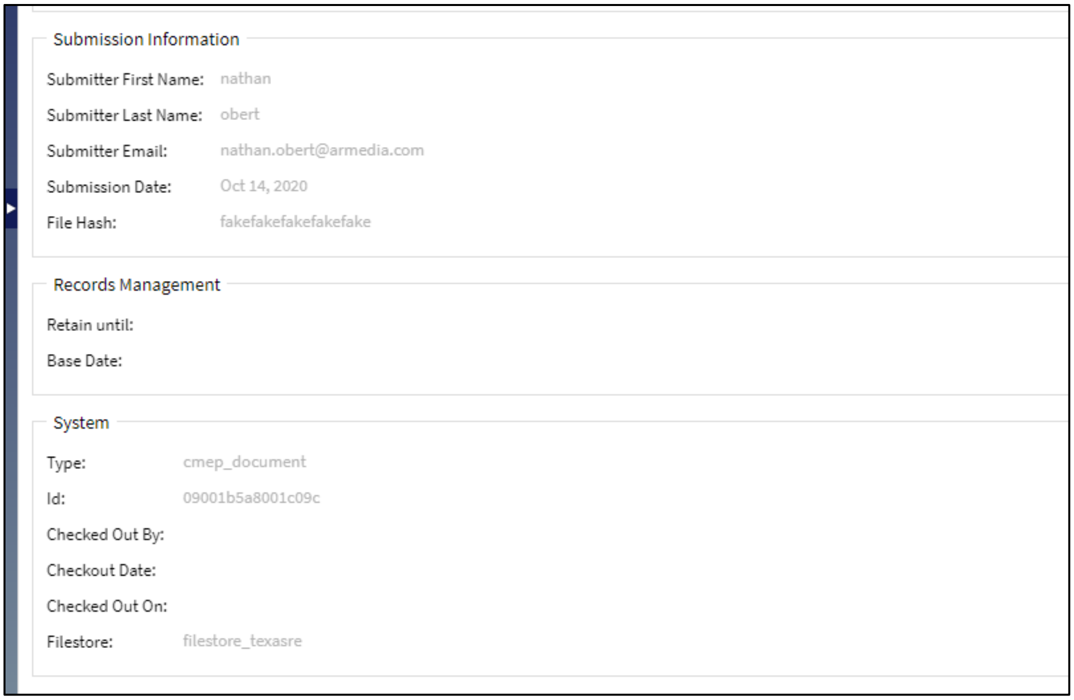
Standards

Standard Requirement: standard 12345
Standard Name: standard
Requirement Number: 12345
Parts: 1

Note that the first tag for every document is its activity number.

Scroll to see the sections for:

- Submission Information
- Records Management
- System Information



Submission Information

Submitter First Name: nathan

Submitter Last Name: obert

Submitter Email: nathan.obert@armedia.com

Submission Date: Oct 14, 2020

File Hash: fakefakefakefakefake

Records Management

Retain until:

Base Date:

System

Type: cmep_document

Id: 09001b5a8001c09c

Checked Out By:

Checkout Date:

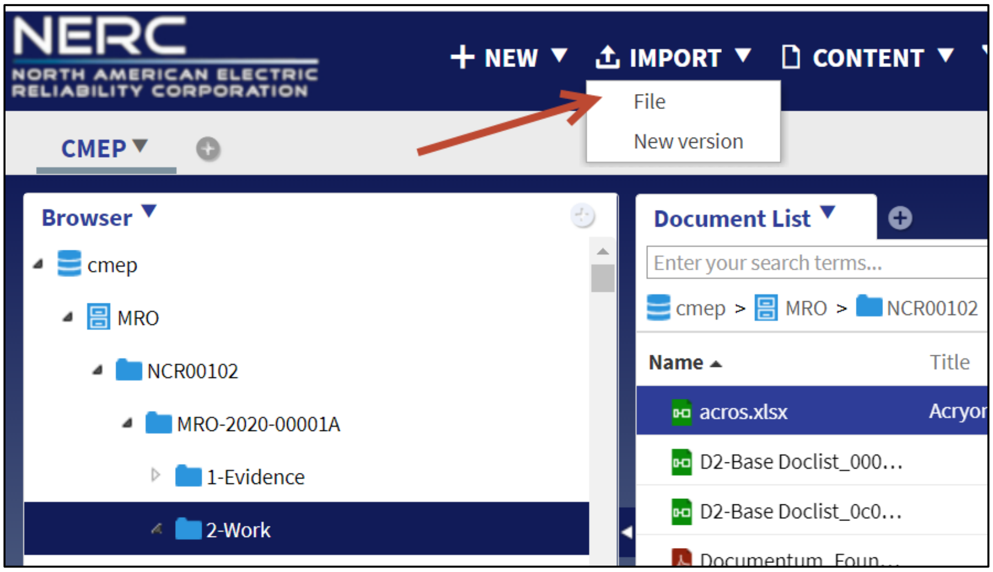
Checked Out On:

Filestore: filestore_texasre

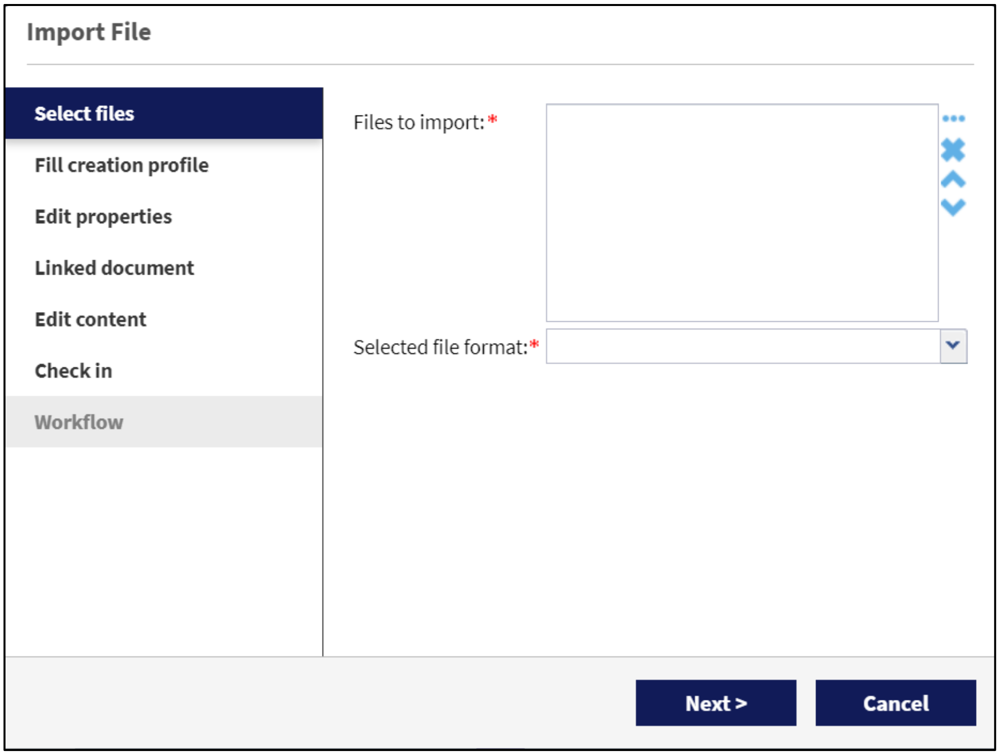
Add a Document

To add a document:

1. Navigate to the Region, Entity, and Activity for the document.
2. Expand the **Activity**.
3. Choose the **Work** folder.
4. Click **Import.**
5. Choose File.



6. The Import File popup opens.



7. Click the ellipsis (**...**) to the right of the file field and navigate to the file or folder you want to add.

NOTE: You can also drag and drop files into the field.

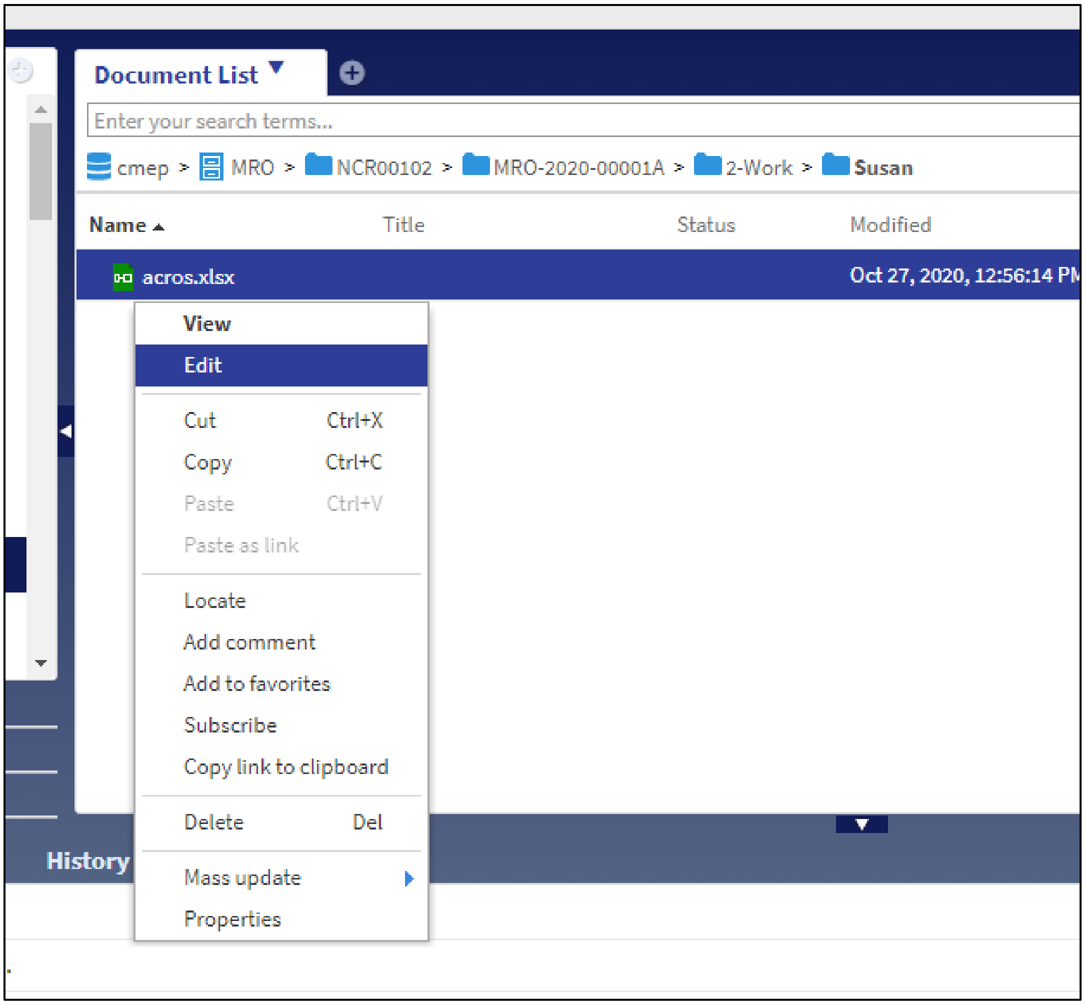
8. Select the file. Edit properties for the file:
   - Title
   - Tags
   - Standards
   - Requirement Number
   - Parts.

When you are finished editing properties the file is added.

Edit a Document

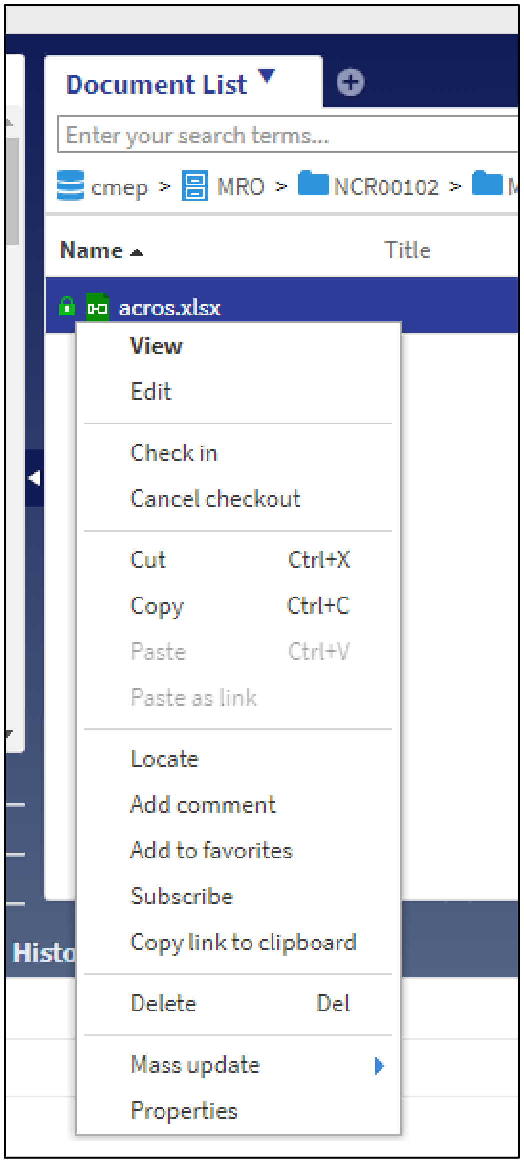
Working documents that are not records or evidence can be edited.

1. Navigate to the document.
2. Right-click on the file name.
3. Select **Edit.**

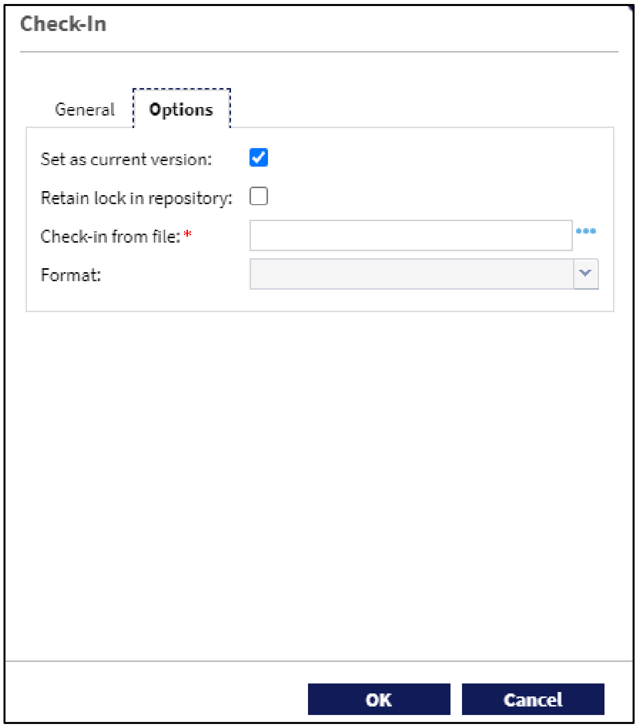


The document downloads to your VDI.

4. Edit the document as you normally would, then save it.
5. Right-click on the file name of the checked-out document.
6. Click Check-in.



7. Select the edited document.
8. Choose the type of version (*0.n* for minor or *n.0* for major) for the document.
9. Select the **Options** tab.
10. Select **Check in from file**.



Check-In

Set as current version: ☑

Retain lock in repository: □

Check-in from file: *

Format:

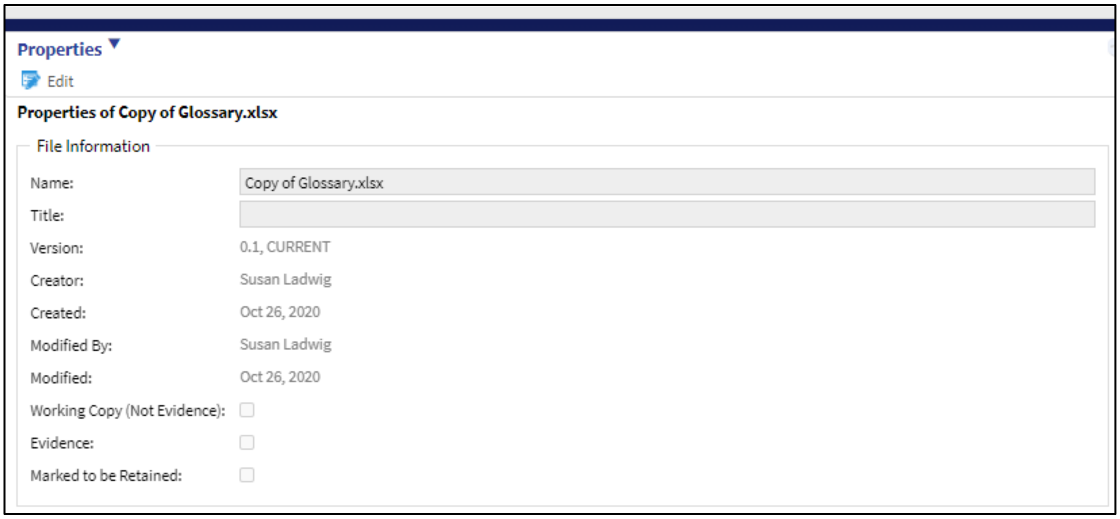
11. Select the ellipsis (…)
12. Navigate to the edited document.
13. Click OK. The new version is uploaded and the version is updated as indicated.

View/Edit Metadata for File

If you have the correct permissions, you can edit file metadata. See the section on Access in the Overview for details.

To edit a file’s metadata:

1. Navigate to the file.
2. Select it. The Properties panel at the right will display the document metadata.



Properties of Copy of Glossary.xlsx

File Information

Name:	Copy of Glossary.xlsx
Title:	
Version:	0.1, CURRENT
Creator:	Susan Ladwig
Created:	Oct 26, 2020
Modified By:	Susan Ladwig
Modified:	Oct 26, 2020
Working Copy (Not Evidence):	□
Evidence:	□
Marked to be Retained:	□

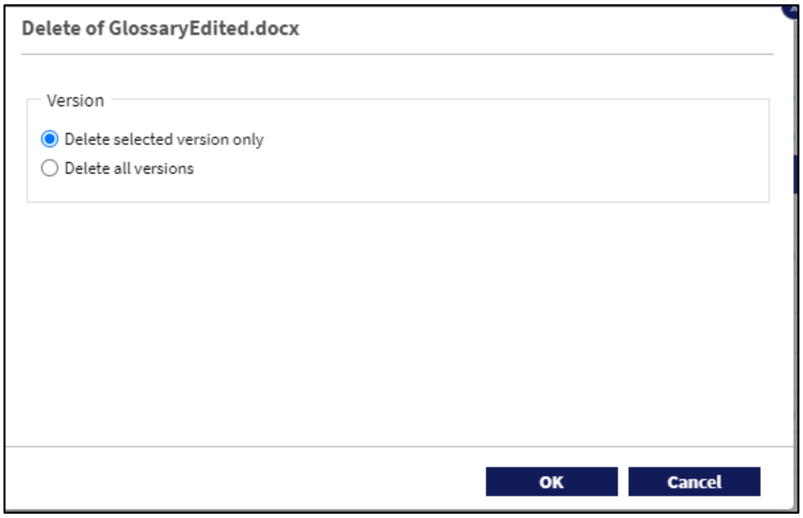
NOTE: You may have to wait or refresh for the newly selected file’s properties panel to display.

3. Click **Edit.**
4. Update the metadata as needed.
5. Click **Save**.

Delete a Document

Custodians can delete any documents that are not records. Analysts can delete their own documents.

1. Navigate to the document you wish to delete.
2. Select it, then press the **Delete** key on your keyboard. The Delete popup opens. Choose the version(s) for deletion. You can delete the selected version or all versions of a document.



Delete of GlossaryEdited.docx

Version

● Delete selected version only
○ Delete all versions

3. Click **OK**.

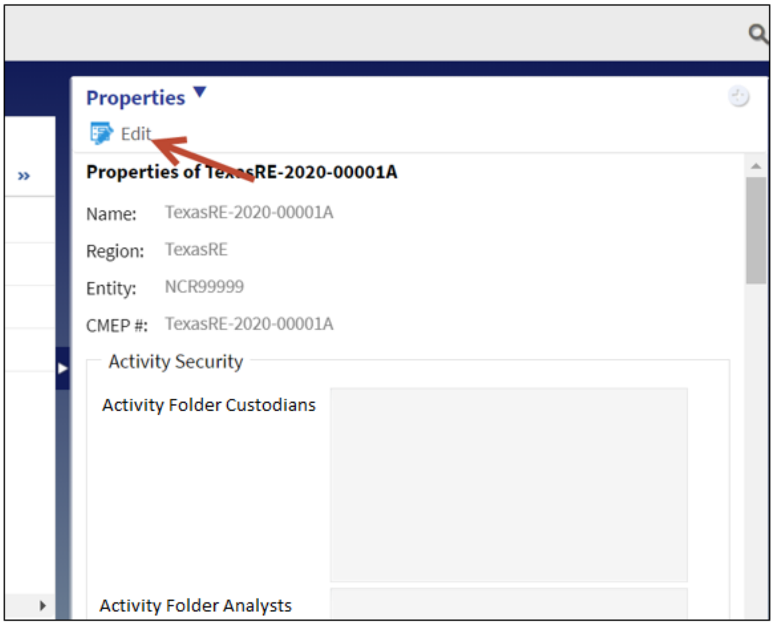
Apply Retention to an Activity

After an activity has been completed, the Activity Folder Custodian reviews the contents and applies a retention policy.

Once the retention policy is applied and started, the records for an activity will be retained for 2 years. Non-records are retained 90 days.

To set retention:

1. Navigate to the Activity to which you wish to apply retention.
2. Select the Activity.
3. On the Properties panel, click **Edit** to open the properties for editing.



Properties of TexasRE-2020-00001A

Name: TexasRE-2020-00001A

Region: TexasRE

Entity: NCR99999

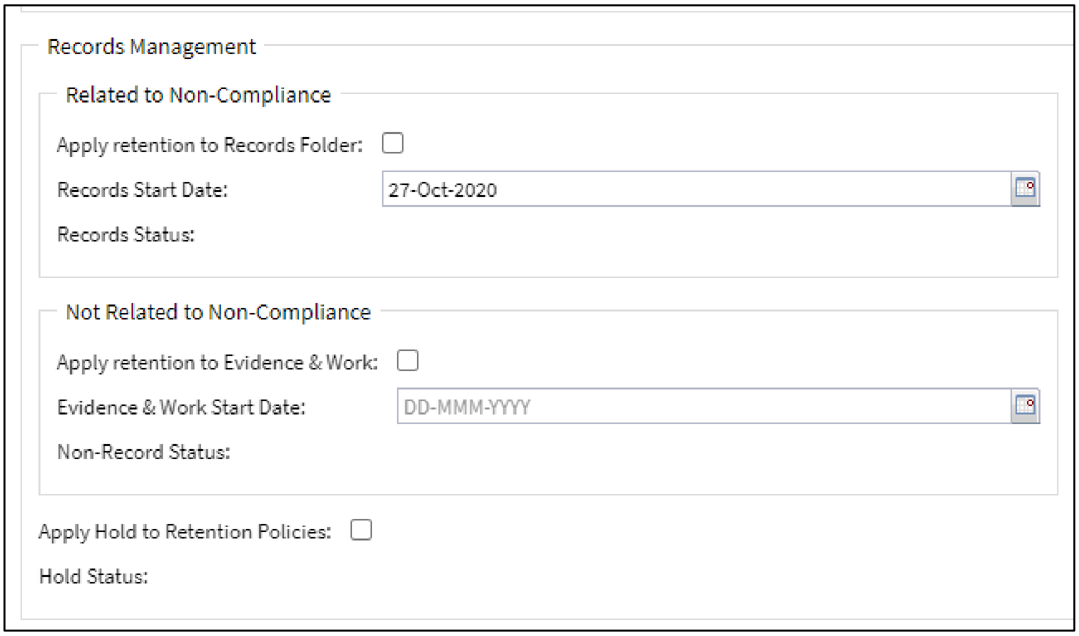
CMEP #: TexasRE-2020-00001A

Activity Security

Activity Folder Custodians

Activity Folder Analysts

4. Scroll to the Records Management section.



Records Management

Related to Non-Compliance

Apply retention to Records Folder: □

Records Start Date: 27-Oct-2020

Records Status:

Not Related to Non-Compliance

Apply retention to Evidence & Work: □

Evidence & Work Start Date: DD-MMM-YYYY

Non-Record Status:

Apply Hold to Retention Policies: □

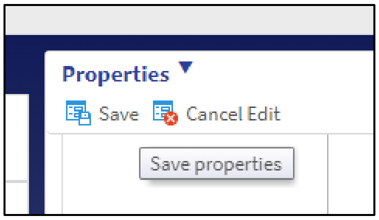
Hold Status:

5. Select the checkbox to apply retention to the Records Folder. The records will be destroyed 2 years from the Records Start Date.

6. If desired, click Apply retention to Evidence & Work. The non-records will be destroyed 90 days after the Evidence & Work Start Date.

7. You can also click the **Apply Hold to Retention Policies** if the activity is on hold. This will prevent the destruction of the records/non-records until the Hold is cleared.

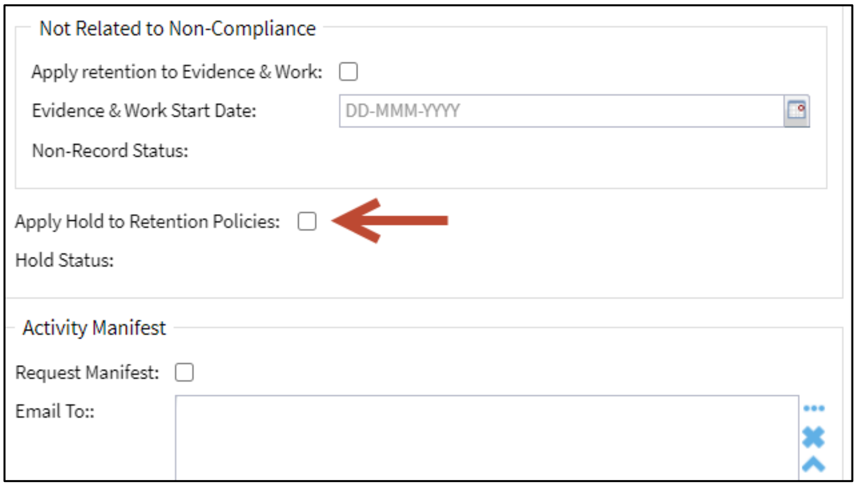
8. When you are done applying retention policies, save the Properties by clicking Save at the top of the Properties panel.



Apply Hold to Retention Policies

If documents that are under retention need to be held (i.e., not destroyed) for some reason such as litigation, you can apply a hold to the activity.

1. Navigate to the activity that is under retention.
2. Click Edit on the Properties panel.
3. Scroll to the Records Management section.
4. Click the Apply Hold to Retention Policies.



Not Related to Non-Compliance

Apply retention to Evidence & Work: □

Evidence & Work Start Date: DD-MMM-YYYY

Non-Record Status:

Apply Hold to Retention Policies: □

Hold Status:

Activity Manifest

Request Manifest: □

Email To::

5. Click **Save**.

This will preserve the documents from destruction until the Hold is lifted.

Remove Hold

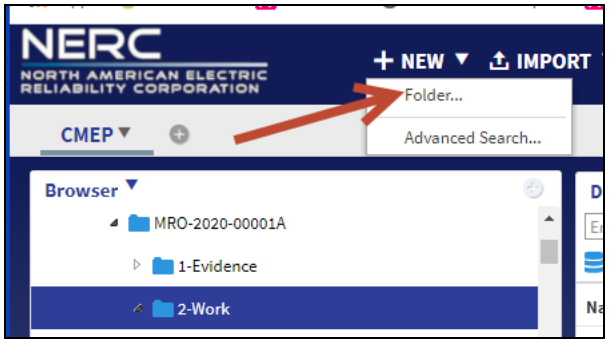
To remove a hold on retained files and allow the retention policy to take effect:

1. Navigate to the activity that is under hold
2. Click **Edit** on the Properties panel.
3. Scroll to the Records Management section.
4. Uncheck the **Apply Hold to Retention Policies** checkbox.
5. Click **Save**.

Create a Folder in the Work Subfolder

To create a folder, for example, a sub-folder in the Work folder of an activity:

1. Navigate to the activity.
2. Select the Activity name.
3. Select the Work folder.
4. Select **New→Folder**.

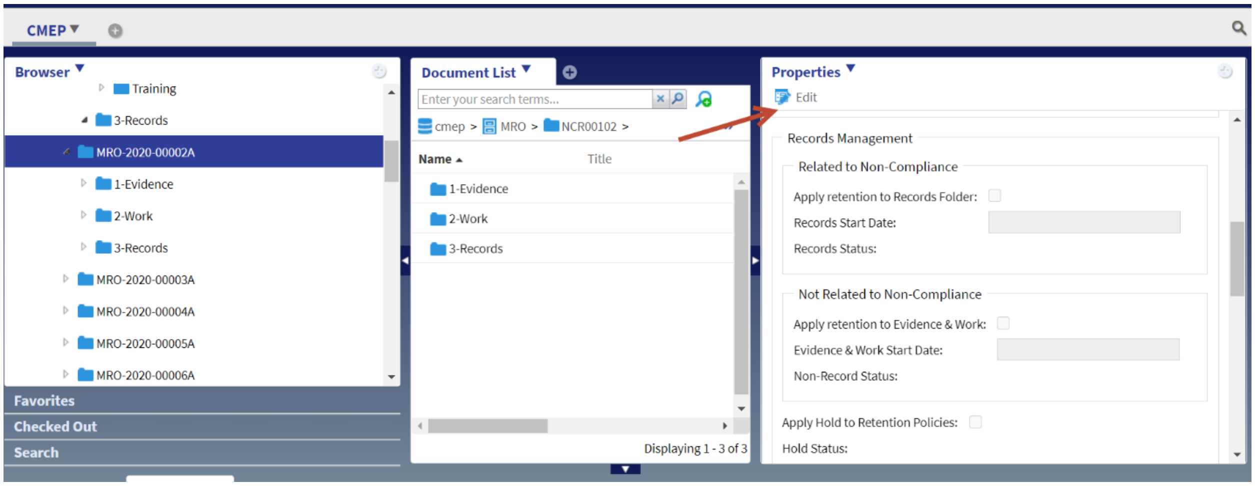


5. Enter the name for the new folder and click **OK.**

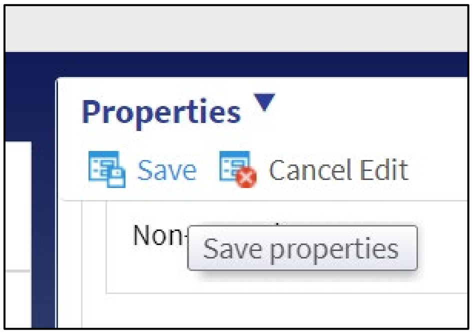
Generate a Manifest

Custodians can send an activity manifest to users with the proper permissions. The manifest is sent as a comma-separated value (csv) file attached to an email. *(Note: manifests can be generated for a specific activity or for an entity. The example below shows manifest generation for an activity. To create a manifest for an entity, the process is very similar, except the user will edit the properties for the entity and all activities within the entity will be included in the manifest.)*

1. Select Browser if necessary.
2. Navigate to the activity and select it.
3. On the Properties panel, select Edit.

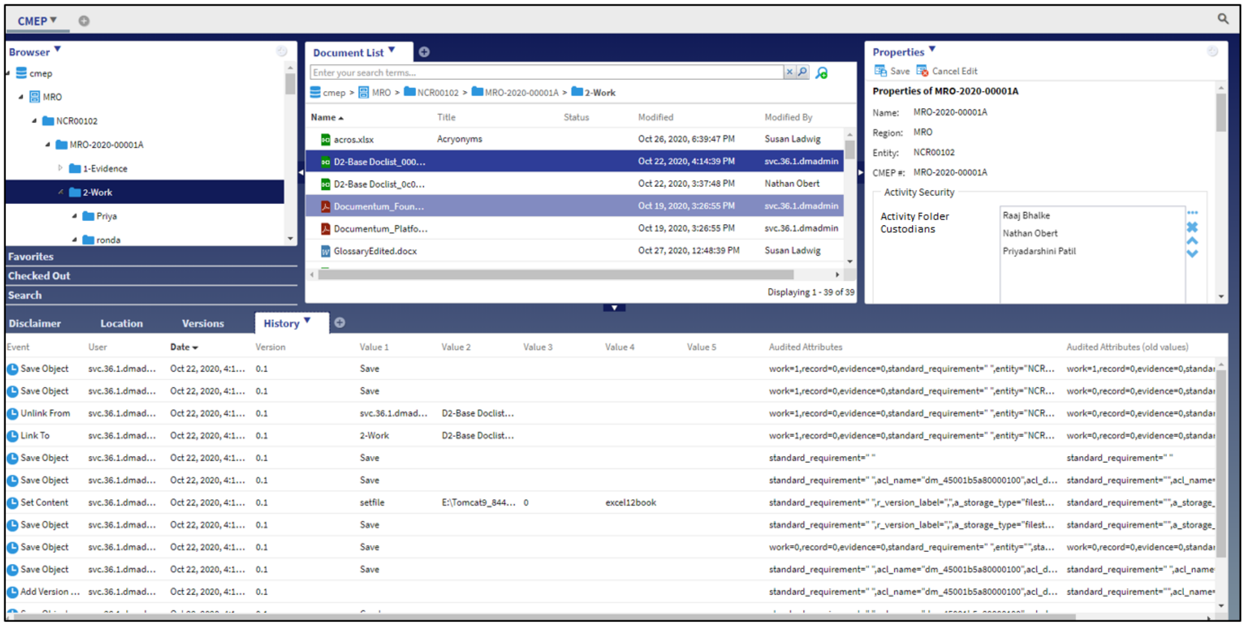


4. Scroll through the properties for the activity to the Activity Manifest section.
5. Click the checkbox for Request Manifest.
6. Click the ellipsis (…) next to the Email To: field.
7. Select the user(s) from the list to receive the emailed manifest.
8. Save the Properties.



History

You can view events related to content by selecting the content, then choosing the History tab. (note: not all users may be configure to view the event History)



Name	Title	Status	Modified	Modified By
acros.xlsx	Acryonyms		Oct 26, 2020, 6:39:47 PM	Susan Ladwig
D2-Base Doclist_000...			Oct 22, 2020, 4:14:39 PM	svc.36.1.dmadmin
D2-Base Doclist_0c0...			Oct 22, 2020, 3:37:48 PM	Nathan Obert
Documentum_Foun...			Oct 19, 2020, 3:26:55 PM	svc.36.1.dmadmin
Documentum_Platfo...			Oct 19, 2020, 3:26:55 PM	svc.36.1.dmadmin
GlossaryEdited.docx			Oct 27, 2020, 12:48:39 PM	Susan Ladwig

Displaying 1 - 39 of 39

Properties of MRO-2020-00001A

Name: MRO-2020-00001A

Region: MRO

Entity: NCR00102

CMEP #: MRO-2020-00001A

Activity Security

Activity Folder Custodians: Raaj Bhalke
Nathan Obert
Priyadarshini Patil

Event	User	Date	Version	Value 1	Value 2	Value 3	Value 4	Value 5	Audited Attributes	Audited Attributes (old values)
Save Object	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	Save					work=1,record=0,evidence=0,standard_requirement=" ",entity="NCR...	work=1,record=0,evidence=0,standar
Save Object	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	Save					work=1,record=0,evidence=0,standard_requirement=" ",entity="NCR...	work=0,record=0,evidence=0,standar
Unlink From	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	svc.36.1.dmad...	D2-Base Doclist...				work=1,record=0,evidence=0,standard_requirement=" ",entity="NCR...	work=0,record=0,evidence=0,standar
Link To	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	2-Work	D2-Base Doclist...				work=1,record=0,evidence=0,standard_requirement=" ",entity="NCR...	work=0,record=0,evidence=0,standar
Save Object	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	Save					standard_requirement=" "	standard_requirement=" "
Save Object	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	Save					standard_requirement=" ",acl_name="dm_45001b5a80000100",acl_d...	standard_requirement="",acl_name=
Set Content	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	setfile	E:\Tomcat9_844...	0	excel12book		standard_requirement=" ",r_version_label=",",a_storage_type="filest...	standard_requirement="",a_storage_
Save Object	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	Save					standard_requirement=" ",r_version_label=",",a_storage_type="filest...	standard_requirement="",a_storage_
Save Object	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	Save					work=0,record=0,evidence=0,standard_requirement=" ",entity="",sta...	work=0,record=0,evidence=0,standar
Save Object	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1	Save					standard_requirement=" ",acl_name="dm_45001b5a80000100",acl_d...	standard_requirement=" ",acl_name=
Add Version ...	svc.36.1.dmad...	Oct 22, 2020, 4:1...	0.1						standard_requirement=" ",acl_name="dm_45001b5a80000100",acl_d...	standard_requirement="",acl_name=

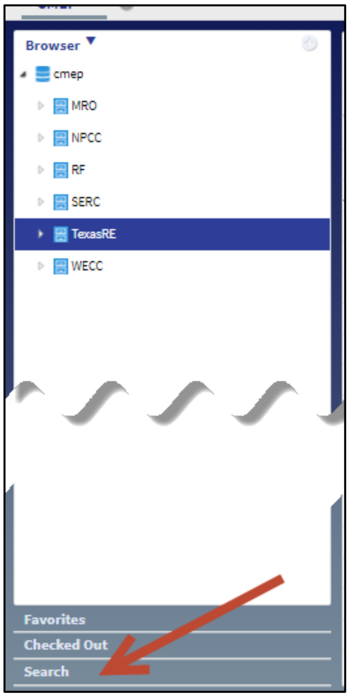
Tips for Using NERC SEL Documentum D2

Searching for Content from an Email Notification

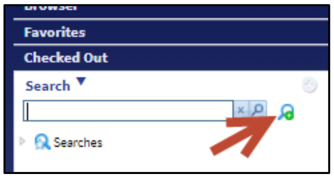
When you are granted permission to access content in the system, you will receive an email with the title of the activity, for example, *TexasRE-2020-00006A*.

To locate the activity in the NERC SEL system:

1. Click on Search.

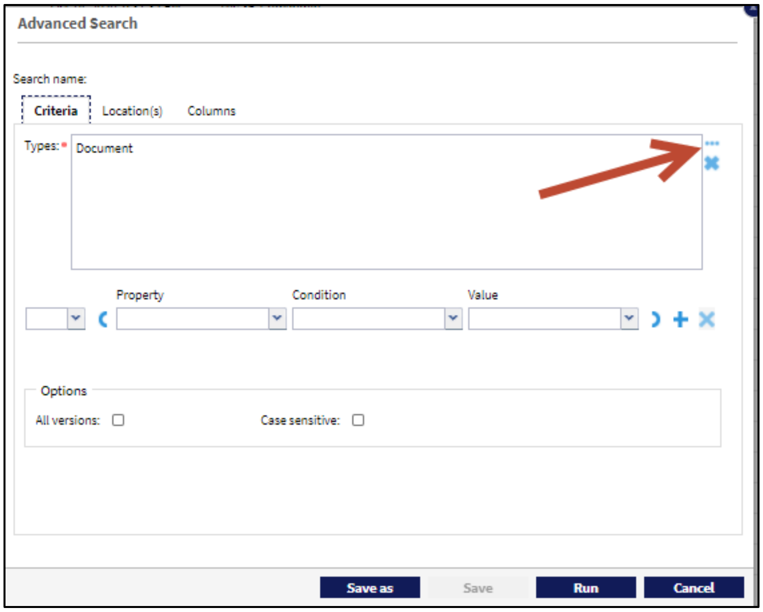


2. Click on Advanced Search.

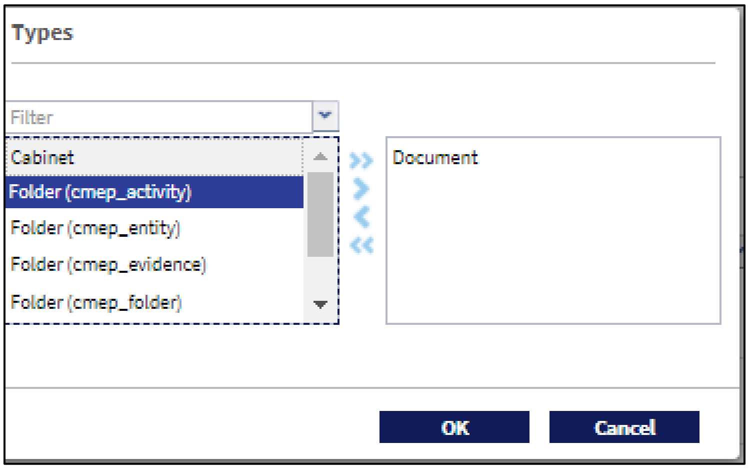


The Advanced Search popup opens.

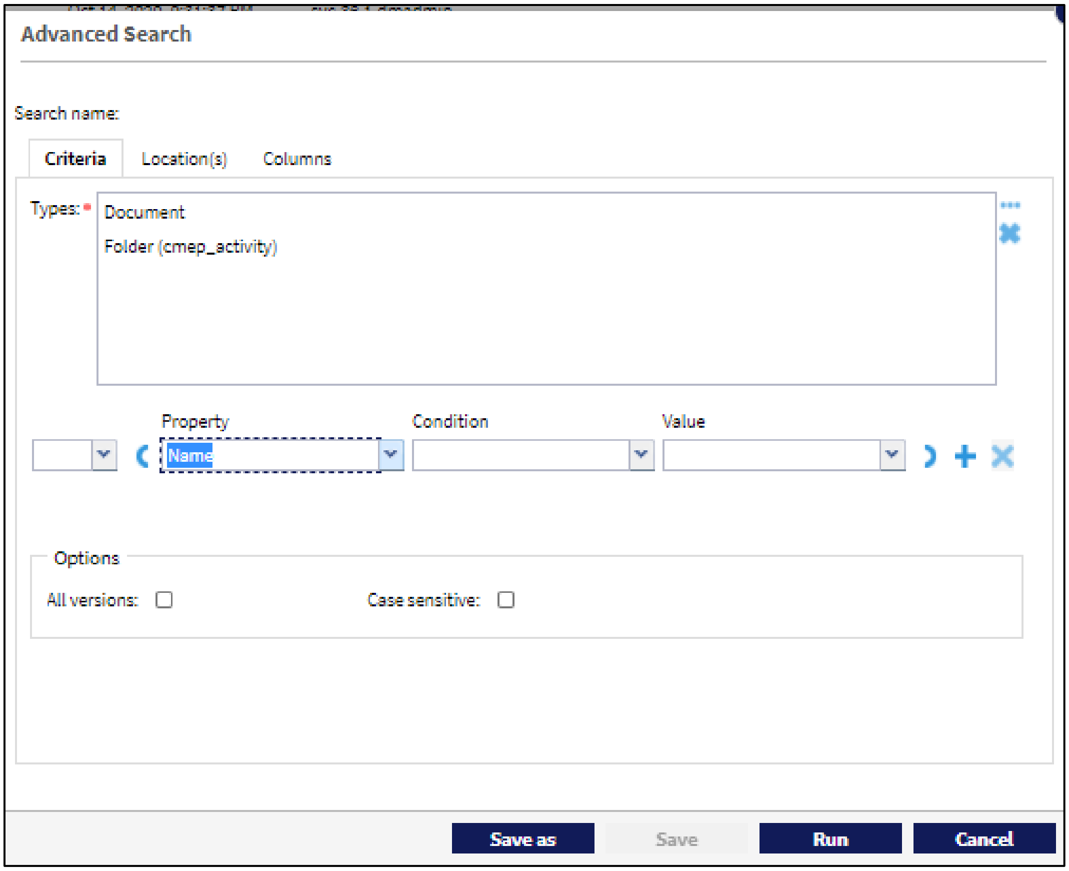
3. Click on the ellipsis (…).



4. Choose the value Folder(cmep_activity) and move it to the right hand column.
5. Click OK.



6. On the search criteria field for Property, select Name.
7. Select Condition = (equals).
8. In the Value column, paste the value from your email.



Types: Document
Folder (cmep_activity)

Property: Name
Condition:
Value:

All versions: □
Case sensitive: □

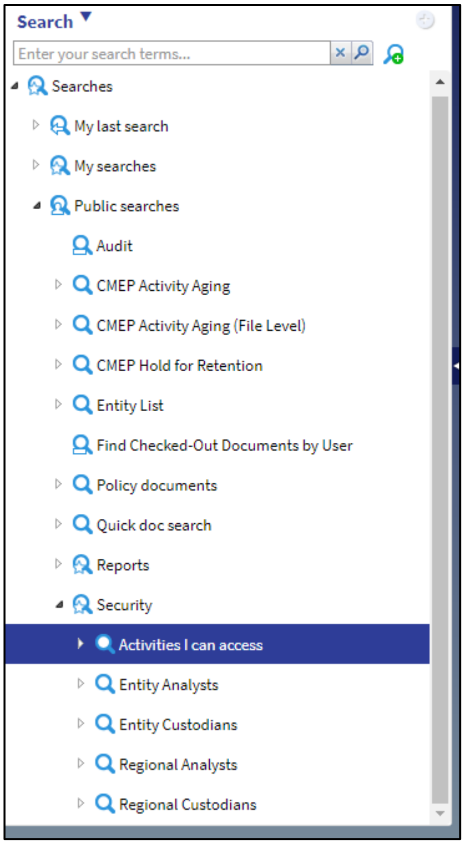
9. Click **Run**. The match is returned.

TIP: Right-click on the activity name and click **Add to Favorites** to locate it quickly the next time.

Locate Your Activities

As you use the NERC SEL system, you will need to locate activities that you have access to. To quickly locate the activities you can work on:

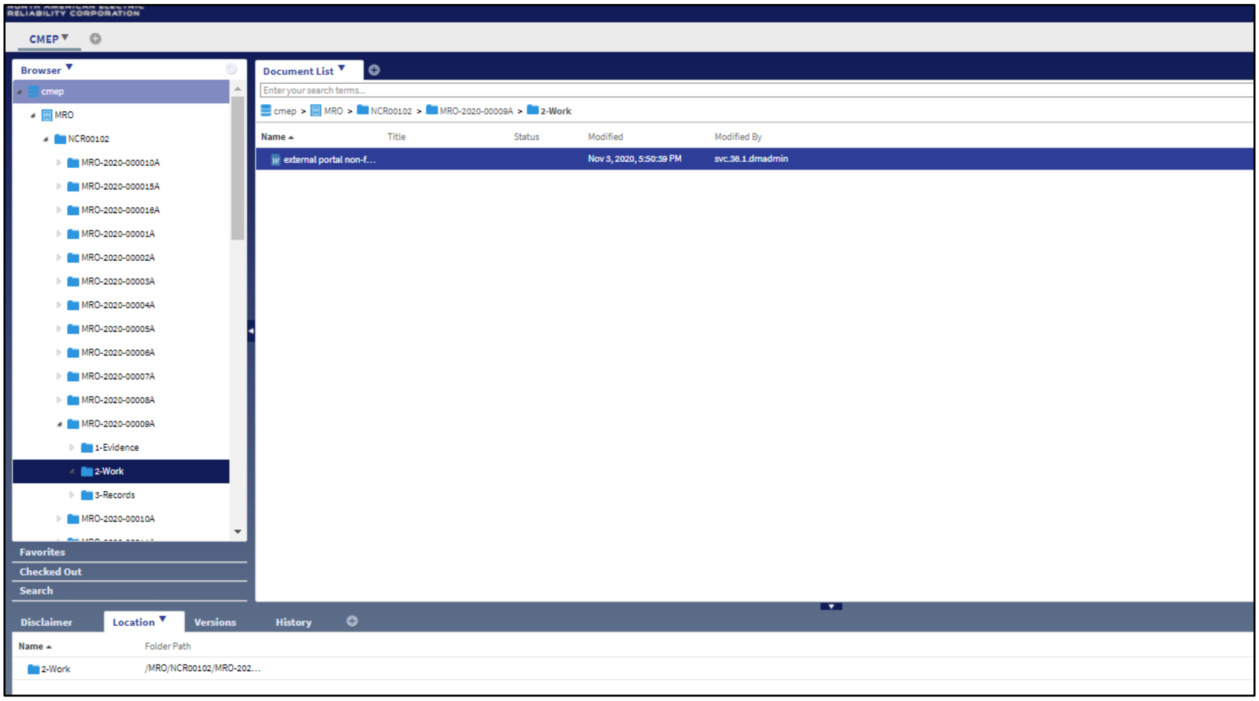
1. Select the Search function from the left-hand menu.
2. Expand **Public searches**.
3. Expand **Security**.
4. Choose **Activities I can access**. A list of activities will be displayed. Choose one to work on it.



Find the Location of a File

To locate the path (entity, activity, and folder) of a particular file:

1. Click on the file name.
2. On the bottom of the page (default layout), view the Folder Path. Hover your mouse over the path to see the entire value. To go to the folder, right click on the name and choose Locate.



Name	Title	Status	Modified	Modified By
external portal non-f...			Nov 3, 2020, 5:50:39 PM	svc.38.1.dmadmin

Name	Folder Path
2-Work	/MRO/NCR00102/MRO-202...

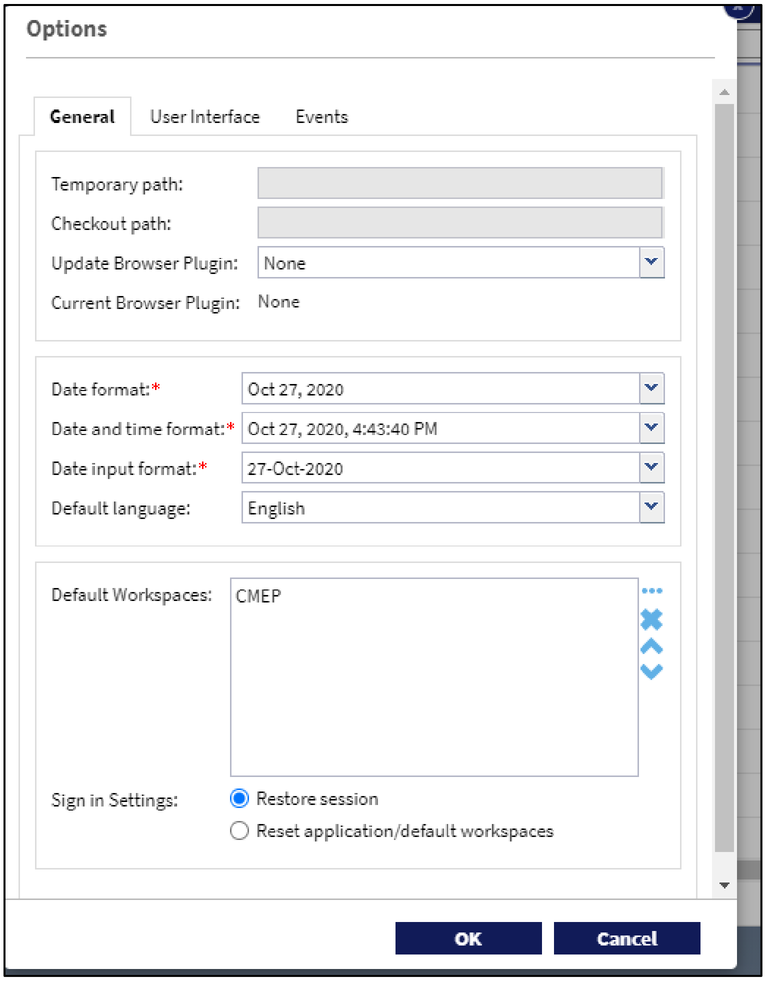
How to Reset Your Workspace

As you are working in the system, you may intentionally or accidentally move or hide a widget that you need to see, or add a widget that you do not want.

NOTE: This user guide reflects the default layout.

You can quickly reset your workspace as follows:

1. Click on your user name and locate the User Settings function.
2. Select **User Settings**.
3. On the Options popup, scroll to the bottom and click **Reset application/default workspaces**.
4. Click **OK**.



Options

Temporary path:

Checkout path:

Update Browser Plugin: None

Current Browser Plugin: None

Date format:* Oct 27, 2020

Date and time format:* Oct 27, 2020, 4:43:40 PM

Date input format:* 27-Oct-2020

Default language: English

Default Workspaces: CMEP

Sign in Settings:
● Restore session
○ Reset application/default workspaces