CA Output Management Web Viewer

Administration Guide

Release 12.1.00

ca technologies

CA Technologies Product References

This document references the following CA Technologies products:

- CA ACF2™
- CA Bundl®
- CA Dispatch™
- CA Deliver™
- CA DRAS
- CA Top Secret®
- CA View®
- CA Spool™

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Overview 9

Audience 9

Chapter 2: Administering 11

Administration Overview 11
Managing Repository Objects 12
- Create a Repository Object 13
- Add Owner Roles to a Repository 14
- Understanding Report Access 15
- Using Owner Roles with Repositories - Overview 15
- How to Customize a Repository Object 17
- DRAS Load Balancing 25
- Using AFP Transform 25

Managing Role Objects 26
- How CA OM Web Viewer Uses Roles 29
- How Role Hierarchies Work 30
- Understanding Role Types 31
- View the Roles in Your System 33
- Create a Role 33
- Create a Subrole 34
- Edit Role Properties 35
- Role Authentication 36

Managing User Authentication 48
- Mainframe Authentication 49
- LDAP Authentication 50
- External Security EXIT 53

Managing Profile Objects 56
- Creating a New Profile Object 57
- Listing Profile Objects 58
- Profile Security and Auditing 59

Managing User Objects 60
- User Object Properties 61
- Creating a New User Object 63
- Finding a User in the User List 64

Managing Directory Objects 64
- Create a Directory Object 65

LDAP Distinguished Name Setup and Usage 67
Managing Subscriptions 68
Favorite Types 68
Create a Subscription Using Favorites 73
Assign a Subscription to a Role - Overview 75
Delete a Subscription from a Role 78
How Subscriptions Are Displayed 79
Report Actions from the Subscription List 79
Managing Preferences 80
Setting General Preferences 80
Setting Display Preferences 85
Setting Output Defaults 87
Setting Auditing Preferences 96
Statistics 99
Exporting and Importing Admin Settings 99
Export Admin Objects 100
Import Admin Objects 101
Import Users 102
Import CA Output Management r11.5 Update 102

Chapter 3: Viewing Web Statistics 103

Viewing Admin Info 104
Viewing the Repository Status 105
Viewing the User Status 107
Viewing the Audit Log 107

Chapter 4: Configuring 111

Managing the Default Repository Filter Settings 111
Update Date and Version Criteria 112
Update Report Criteria 114
Update Index Criteria 115
Managing the Report List Display Settings 117
Update the Report List Layout 117
Show Advanced Options 119
Override Report List Layout Settings 119
Managing the Favorites List Display Settings 120
Update the Favorite List Layout 120
Show Advanced Option for Favorites 122
Override Favorite List Layout Settings 123
Managing the Report Level Actions Settings 123

Configure Report Browsing 124
eMail Type 125
SMTP Email Account 125
Managing the After Login Settings 127
Change User Roles 127
Choose a Repository 128
Show Repository List 129
Managing Your Credentials 130
Set the Default and Individual Credentials for Repositories 131
Restore Your Credentials 131

Chapter 5: Frequently Asked Questions 133

FAQs 133

Index 139

Chapter 1: Overview

This section contains the following topics:

Audience (see page 9)

Audience

CA OM Web Viewer lets you view documents in a web browser that CA Output Management Products manage on your mainframe system. This guide describes setting up your report viewing network, defining roles, repositories, profiles, subscriptions, User IDs and all the processes and required objects to view your mainframe reports online in your browser.

Important! This guide is intended for System Administrators who manage user permissions to view and use documents, department-wide, or enterprise-wide.

Note: This guide assumes that you are familiar with mainframe security and report administration within your user mainframe repositories. For example, CA Dispatch, CA Deliver, CA View, and CA Spool.

Chapter 2: Administering

This section contains the following topics:

Administration Overview (see page 11)
Managing Repository Objects (see page 12)
Managing Role Objects (see page 26)
Managing User Authentication (see page 48)
Managing Profile Objects (see page 56)
Managing User Objects (see page 60)
Managing Directory Objects (see page 64)
Managing Subscriptions (see page 68)
Managing Preferences (see page 80)
Exporting and Importing Admin Settings (see page 99)

Administration Overview

To set up and manage CA OM Web Viewer objects, use the Administration tab and the following object subtabs:

Repository

References a mainframe repository (CA View, CA Dispatch or CA Bundl).

Most properties that you set at the repository level lets you limit or change the access of the users who view and use the reports and data in the repository.

Role

Provides a definition of permissions. You can use a role to group users together to make the assignment of privileges less labor intensive. Roles are used to specify permissions for:

- User Authentication Type
- Ability to use email, save, print, and export report actions with option page limits
- Enable and disable favorites selections
- Determine the subscriptions and subscribed reports available for anyone that is defined with this role

Profile

Provides a definition that lets multiple LDAP users log on to CA View or CA Bundl using a single administrator-defined set of mainframe credentials. A profile can also provide the same user-entered LDAP credentials are mainframe credentials.

Notes:

The special LDAP Mainframe Hybrid Profile Object forwards the LDAP credentials of the user to mainframe security.

The special External Security EXIT Profile Object means the mainframe profile obtained via exit calls.

User

Provides basic user information, including the selected roles for this user.

Directory

Provides the LDAP information that validates a group of users with your current LDAP system.

Note: The special EXIT directory Object means the user directory system defined externally to Web Viewer.

Preferences

Includes General and Display preferences, output defaults, auditing settings, and statistics.

Note: Group Administrators can only access the Role, Profile, and User options, but System Administrators have access to all the admin options.

Managing Repository Objects

Repository objects are a reference or connection to a mainframe (CA View, CA Dispatch, or CA Bundl) repository. You view, create, edit, and delete the repository objects on the Repository subtab of the Administration tab. You can click the Name column header to sort the objects by the repository name in alphabetic or reverse alphabetic order. You can also refresh this list from the CA OM Web Viewer database.

A number of properties are controlled at the repository level. These properties let you control the abilities of all the users who have access to this repository object. For example, you can have certain roles that only have access to a particular repository object.

Consider the following information about repository objects:

- Each repository object maps to exactly one CA View, CA Dispatch, or CA Bundl system. A repository object can *never* map to two different repositories
- You can create several different repository objects that each point to the same View, Dispatch, or Bundl repository location, but have different access permissions.

  For example, you can have two or more repository objects that point to the same View repository, so that different independent groups of properties can be applied to different roles/users. Therefore, you could have two repository objects that both point to the same mainframe repository, and have one repository object that allows the file upload, and one repository object that does not allow a file upload.

Create a Repository Object

You create a repository object...

Follow these steps:

1. From the Administration tab, click the Repository subtab.
2. Click Create.
3. Complete the following required fields:
   - Enter a Repository name that refers to the repository that you want to reference; recognizable to the users who have to find that Repository.

     For example, you enter **West Coast CA View** to provide geographical and product information about this repository.
   - Select CA View, CA Dispatch, or CA Bundl as the Repository Type.

     The available Repository Locations list will show only repositories of the type you select. For example, if you select CA View, no CA Dispatch or CA Bundl repositories will be listed as possible repository locations.
   - Select a Repository Location.

     The location address consists of a mainframe system ID, a DRAS system, and either a CA View, CA Dispatch or CA Bundl system.

     For example:

     ENFSYSID:DRASA:SALESVW or ENFSYSID:DRASB:SALESBDL

     You can refresh the list of choices with the DRAS Discovery button.
   - From the Available Roles list, select the Roles that are to have access to this Repository and move them to the Selected Roles list.

     For example, you assign System Admin and East Coast Group Admin.
4. Click Create.

   The repository object is created with your basic required settings.

Add Owner Roles to a Repository

You can add owner roles to a repository.

Follow these steps:

1. From the Administration tab, click the Repository subtab.
2. Select your repository.

   The edit Repository object panel displays.
3. On the Definition tab, find the Owner Roles section:

   You view the Available Roles and Selected Roles lists.
4. Select one of more names in the Available Roles list.

   Hold Ctrl or Shift while clicking to select more than one Role
5. Click the single right arrow between the two lists to add the selected Role (s)
6. (Optional) Click the double right arrow to add all the Roles to the Repository.

   All of the Roles in the Selected Role list can now have the possibility of accessing this Repository. See the explanation above for other limitations on Repository access.
7. Click the Update button near the top right of the panel.

   The Roles are added.

Roles can also be given access to a repository at the Roles panel. However, the System Administrator role cannot be edited from the Role panel. To add the Systems Administrator role to a repository, it must be added from this panel.

Understanding Report Access

Just because a role has access to a repository, does not necessarily mean that every user in that role can view every report in that repository. Limiting the access of a role to repositories is one of several ways of limiting access to reports in CA OM Web Viewer and the base repository systems.

Limiting Report Access through Mainframe Repository Security

In order for a user to see report information, their mainframe account, or proxy profile must have access to the report in the base CA View, CA Dispatch, or CA Bundl system.

Report access can be further limited within the security setup in the mainframe repositories. Be aware that CA OM Web Viewer users cannot access reports that they are not, or their Profile is not allowed to access through the mainframe system.

For more information on controlling user access within the base CA View, CA Dispatch, or CA Bundl systems, see the product documentation for those products.

Note: As a work-around, set up a profile account that has access to a report in which the user would not normally have access.

Limiting Report Access Thorough the Use of Subscriptions

Report access can be further limited with subscriptions in CA OM Web Viewer. Basic User roles only let their users access reports assigned to the role with the subscriptions.

Notes:

- The repository that the report is in must also be assigned to the role.
- If the user can have access to more than one role, they can access other reports; the reports available to the other roles.

Using Owner Roles with Repositories - Overview

Owner Roles refer to any Roles that are allowed to access this Repository. There may be situations where only certain Repositories need to be available to a Role.

Depending on how your reports are divided between your Repositories, it might make sense to only allow a certain Role to access certain Repositories. For example, if all your sales Reports are in a certain Repository, the Salesman Role would be allowed access to that Repository. Additionally, the Salesman Role might not be allowed to access a Repository with accounting information stored in it. A Repository maps to exactly one CA View, CA Dispatch, or CA Bundl system.

Just because a Role has access to a Repository, does not necessarily mean every user in that Role can view every Report in that Repository. Limiting a Role's access to Repositories is one of several ways of limiting access to reports in CA OM Web Viewer and the base Repository systems.

In order for a user to see report information, their mainframe account or proxy profile must have access to the report in the base CA View, CA Dispatch, or CA Bundl system.

Report access can be further limited within the mainframe repositories. Be aware that Users cannot access reports that they are not allowed to access through the mainframe system. One work-around for this is to set up a Profile account. See the Profiles section for more information.

Example

If Advanced Users, Group Administrators, and System Administrators have a repository object assigned to their role, they can view any report in the base system of that Repository object that their mainframe credentials would normally have access to in the base CA View, CA Dispatch, or CA Bundl system.

Be aware of the following additional factors:

- Report access can be further limited with Subscriptions in CA OM Web Viewer. Basic User Roles only allow their users to access reports assigned to the Role with the subscriptions they are to be able to view. (See Role - Assigning Subscriptions to a Role)

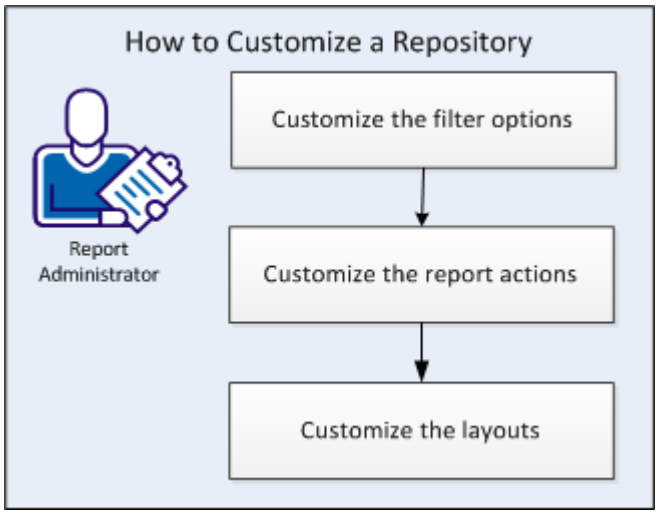
  However, to view a report, even if the report has been assigned with a subscription to the user's Role, that user's Role has to have access to the Repository where the report resides, to view the Report. Basically, both have to be true; the report must be assigning in a subscription to the Role, and the Repository the report is in must also assigned to a user. (See Subscription – TODO exact place)

- Roles can also be given access to a Repository at the Roles panel. (See Assigning Repositories to a Role) However, the System Administrator Role cannot be edited from the Role panel; so to add the Systems Administrator Role to a Repository it must be added from this panel.

How to Customize a Repository Object

As a Report Administrator, you want to customize repository objects. For example, you want to customize the views of the reports that reside in a repository. You also want to customize the actions that you can perform on the repository objects.

The following diagram shows you how to customize repository objects:



1. Customize the filter options (see page 18).
2. Customize the report actions (see page 21).
3. Customize the layouts (see page 24).

Customize the Filter Options

The Filter Options panel lets you select filters that apply to the selected repository. For example, you can limit the maximum number of days that a user can search.

Follow these steps:

1. Select any of the following date filters and click Update:

   Default relative date filter setting

   Sets the number of days that appear by default in the report search filter for this repository.

   For example, if you specify 3650 days, when you go to the Advanced Search and click on this Repository, the default search criteria listed shows 3650 in the days ago column.

   Default: 9999 days

   Note: End users can override this setting by updating the Default Filter Settings in the Configuration tab.

   Date filter warning threshold

   Displays a warning message if the date you entered for the report search specifies a range that is too large. A very large date range can cause slow response times. This setting only warns the users if the searches are likely to cause slow response times, but you can limit the user with the maximum date filter range setting.

   Default: 0 days; meaning no warning threshold.

   Note: This setting applies to both the Days ago filter, and the Date range filter. If the System Administrator sets a limit of 300 days, users will get warned if they use a number larger than 300 in the Days ago field, or if the dates in the date range are more than 300 days apart.

   Maximum date filter range

   Sets an upper limit on the number of days that a user can search at one time from the advanced search panel. The same value applies to the Cross-Report Index searches. If a user tries to search for larger number of days' worth of reports or cross-report indexes, a message displays that indicates a search for that many days cannot be performed.

   This setting applies to both the days ago filter, and the date range filter. If the Systems Administrator sets a limit of 365 days, the user will not be allowed a number larger than 365 in the days ago field, and the dates in the date range cannot be more than 365 days apart.

   Default: 10000 days

2. Select a wildcard user restriction from the name filters to control whether your users can insert leading asterisks in searches, and click Update:

   None

Let the user specify a leading asterisk in searches.

Warn on leading asterisk

Sends the user a warning when using a leading asterisk.

Disallow on leading asterisk

Does not let the user specify leading asterisks to search for terms.

Note: These leading asterisk options apply to the Report ID criteria in the advanced search Report List and Cross-Report list.

3. (Optional) Select to enable or disable Display Mode and DistID (CA View only):

Enable

Let users search for reports associated with any mode and distribution ID that they choose.

Disable

Limits the search for only reports within the current Mode and Distribution ID of the user, determined by the current setting within that CA View repository.

Notes:

- In no situation are users allowed to select a mode or distribution ID that they do not have access to in the CA View repository.
- Mainframe credentials are used to access the base CA View repository, whether they come from a profile in the case of certain LDAP or EXIT users, or from the user directly.

4. (Optional) Enable index value filter rules to reduce the search time for certain common index searches. These rules help users avoid certain types of searches that would take longer; and these rules can help set up similar, faster searches that also return the desired results.

   Note: The rule applies only to a specific index that was created for this Repository.

5. Consider the following information about these rules:

   - Rules can stop or limit the user from using wildcards.

     For example, if a user enters an index value using a leading asterisk wildcard rather than the needed leading zeros, the response time may be unnecessarily long.

     If there is a large number of indexed reports and values, a search for *13 takes longer than 000000013.

   - Rules can format certain entries with auto-padding automatically to produce an index value of the correct format.

     For example, with the correct rule, a user might only enter **345**, and the rule corrects the number of leading zeros automatically to make this a ten digit account number: 0000000345.

     The fields created by these rules are what is actually sent to the CA View, or CA Bundl system, when a search is performed for an index value. A rule is constructed of several attributes set from the Rule List table.

   - In addition to setting user limits, rules also reduce the number of keystrokes required. Since the index values use a specific format, these rules reformat the values entered by a user to the correct values.

Customize the Report Actions

The Report Options panel lets you set properties and actions that involve accessing or viewing a report:

- Transform AFP Report
- Offline Report Access
- Report Action
- File Upload

Follow these steps:

1. Select one of the following Transform AFP Report options and click Update:

   Keep as AFP

   Sends all AFP reports directly to the end-user computer in AFP format.

   Convert to PDF

   Converts all AFP reports to PDF reports before it sends to the end-user computer.

   User Choice (AFP or PDF)

   Let the user determine whether APF reports convert to PDF reports using the setting on their user configuration tab.

2. Set up offline report access.

   Notes:

   - These settings are only applicable for CA DRAS repositories that support the recall functionality.
   - The last two options require system setup in your existing mainframe system.

   Disable recall of off-line reports

   Select this option if the repository does not support recall through DRAS or you want to disable recall by CA OM Web Viewer users.

   Recall reports from off-line media

   If supported, you can request the recall of offline reports.

   Note: Recall only works with a CA Dispatch or CA View system that has recall automation implemented.

   View reports from off-line media without recall

   If supported, and you have EAS or Centera access enabled through CA View, you can view offline reports without recalling them.

3. (CA View only) Enable or disable comment updates and click Update.

With this option, selected users with a role type of Advanced User or higher can edit the report comment in this repository. The CA View® repository must have compatible settings.

Without this option, no users can edit a report comment in this repository. The CA View® repository does not have to have this option disabled, in order to disable it through this repository in CA OM Web Viewer.

4. (CA View only) Enable or disable annotations.

   If enabled, Basic User type roles can view notes, and higher level role types can perform further actions, depending on the granular settings.

5. Set Specific Annotation Permissions.

   These options control the default type of new notes, and can also limit a user to being able to create only public or private notes:

   Default to public

   Create public or private annotations and set public as the default.

   Default to private

   Create public or private annotations and set private as the default.

   Public only

   Create public annotations and set the default option for a new annotation to public.

   Private only

   Create private annotations and set the default option for a new annotation to private.

6. Set permissions for users to delete annotations.

7. Set permissions for updating notes and creating bookmarks.

   Note: Regardless of these settings, only users with a Role type of Advanced User, Group Administrator, or Systems Administrator are able to add bookmarks, because basic users do not have access to bookmarks.

8. Set permissions for upload permissions and distributed file uploads. If your site has CA Spool LPD interface installed on the mainframe, you can give users permission to upload files such as PDF, XLS, and so on to the mainframe. You must have an SAR type LPD queue setup which refers to the repository to which you want to upload files.

   Note: For more information, see the *CA Spool System Guide*.

From CA OM Web Viewer, you must define which text file queue, and non-text file queue is setup for the CA View, CA Dispatch, or CA Bundl system of this repository object. If you decide to allow file upload, and set it up, all users except Basic User role users see a File Upload toolbar on their report list panel. Since this Repository object refers to a particular CA View, CA Dispatch, or CA Bundl system, the queue chosen here should probably refer to the file printer queue for that same system.

Server Name or IP

Specifies the name of the LPD Server.

TCP/IP Port

Specifies the LPD Server port number, usually 515.

Text File Printer Queue Name

Specifies the name of the LPD Text File Printer Queue that is associated with a CA View®, CA Dispatch™, and CA Bundl® repository. You use this queue for all text reports.

Important! The System Administrator must select the correct queue. If the queue points to another system, users can get confused as to where their uploaded files were sent, since their files are in a different repository than the one they were working with when the files were uploaded.

Non-Text File Printer Queue Name

Specifies the name of the LPD Non-Text File Printer Queue that is associated with a CA View®, CA Dispatch™, and CA Bundl® repository. You use this queue for all non-text reports.

Important! The System Administrator must select the correct queue. If the queue points to another system, users can get confused as to where their uploaded files were sent, since their files are in a different repository than the one they were working with when the files were uploaded.

Customize the Layouts

Design the way that you want to display report information. You can customize the layouts of the Favorites and Report lists, and selected report sort columns.

Follow these steps:

1. Set the Report List Layout for the default report list, and click Update.

   For example, you want to add attribute columns to the Selected Reports Columns in the Report List layout.

   Note: Changing these settings affects the Report List and the Cross-Report Indexes list under the Advanced Search tab. The Favorite List Layout affects only the Favorites subtab under the Advanced Search tab.

2. Set the Favorite List Layout for the Favorites List, and click Update.

   For example, you want to change the attribute columns that users see by default and the default order of the columns.

3. Select a column to define the default sort-by column, for each list.

You have successfully customized a repository object.

Notes:

- The original settings are only the defaults, and users can override these column settings from their Configuration tab.
- The Favorites list, the Report list, and the Cross Report List under the Advanced Search tab all must have at least one of these optional columns included. All other attributes are optional. You can select or not select any of the attributes listed in the Available Report Columns list or the Available Favorite Columns list.

DRAS Load Balancing

CA OM Web Viewer performs automatic DRAS load balancing for users among the available DRAS servers You can set up as many DRAS servers as you require for the size of your user base.

To set up DRAS load balancing, select one or more alternate locations for a repository. You can define these locations so that each repository can be accessed through several different DRAS servers. CA OM Web Viewer distributes users among all the locations that the repository object has automatically.

Consider the following information about setting up your DRAS load balancing:

- Verify that all locations you selected in a repository object point to the same base View, Dispatch, or Bundle repository.
- You must use a different ENF or DRAS address, but do *not* use a different base repository.
- The Available Locations that display in the Alternate Locations section only include likely choices for alternate locations.

Using AFP Transform

For CA View users (with a r11 or newer repository) that has the CA View AFP Transform feature installed and enabled, select the appropriate option. You can transform all AFP reports to PDFs automatically, leave APF reports in the AFP format, or let the user decide whether they want to transform AFP reports to a different format.

Consider the following information:

- This transform option applies to all AFP reports viewed from this repository.
- If you decide to leave AFP reports in AFP format, the user needs an AFP viewer installed on their computer.
- If you let the user decide whether to transform AFP reports, their personal configuration settings controls whether an APF report is transformed to PDF.
- If the repository type is not appropriate or the transform feature is not installed and enabled, this setting is ignored and AFP reports are not converted.

Managing Role Objects

Role objects let you manage system permissions and privileges to define and simplify different access levels. For example, some users require view access to reports that are specific to their job titles. Other users must perform advanced searches and want to create subscriptions (groups of reports) for their teams. A different set of users wants to upload information to a repository. Also, your database and report administrators want extensive access and security permissions to manage the system and everyone who is using it.

The System Administrator or Group Administrator (GA) assigns all privileges and permissions to a role object, not to an individual. The Group Administrator can then assign all those individual users to the role as needed. This action creates a group of people who each have all the system access capabilities that are associated with that role.

CA OM Web Viewer includes only the Default User and System Administrator roles. You can define other role types manually. Although the other role types let you have more than one role object of a particular type, you can only have one *System Admin*.

Default User

If a user with valid mainframe credentials logs in to CA OM Web Viewer, but does not have access to any role, that user logs in using the Default User Role. Also, if the user has not been previously defined, that user has a user object defined automatically, and placed in the Default User Role. For more information, see Auto Enrollment - Mainframe Users.

The Default User Role can have repositories and privileges assigned to it in the same manner as any other role.

System Admin

The System Admin has complete access to the CA OM Web Viewer system. This role cannot bypass existing mainframe repository data restrictions in CA Dispatch, CA Deliver, or CA View.

All future Roles contain a subset of the System Admin privileges. The *System Admin* role is the only role in Web Viewer that can have a role type of System Administrator.

When you install CA OM Web Viewer, you *must* define a default system administrator. This Default System Administrator is the first member of the System Admin Role. You can add other users to the Role later to have more than one user with System Admin privileges.

Administrators design and maintain roles to control user permissions and their access to data, databases, repositories, and reports in the system. You can give an individual user more than one role assignment. For example, you have a Bank Teller role and you assign ten individual Bank Tellers, but you can assign the Bank Manager to a Bank Manager role, and also to the Bank Teller role.

This setup lets the Bank Managers operate with the privileges and data that the Bank Tellers use, but it also allows the manager to access a different set of data assigned to Bank Managers specifically.

Roles make the designation of privileges much less labor intensive:

- You can set or adjust the privileges for hundreds of users at one time by simply modifying the role.
- When the Group Administrator promotes or reassigns a user, they do not have to change privilege. They can simply assign that user to a different existing Role that has all the privileges necessary for the new job.
- You can assign an individual to more than one role.

Functionality	**Basic User**	**Advanced User**	**Group Admin**	**Systems Admin**
LDAP Authentication	Yes	Partial, LDAP Mainframe Hybrid Profile Object Only	No	No
Mainframe authentication (CA Top Secret®, CA ACF2™, RACF)	Yes	Yes	Yes	Yes
View Subscribed Favorites (Report, Report Search Filter, Cross-Report Index-Value Report Section, Report Index and Report Index-Value Report Section))	Yes	Yes	Yes	Yes
Text Find/Go to Page	Yes	Yes	Yes	Yes
Create Browse Favorites or Bookmarks	Yes	Yes	Yes	Yes
Print, Email, Export (the number of pages can be limited)	Yes	Yes	Yes	Yes
Advance Search (Search for unsubscribed reports and Cross-Report Indexes)	No	Yes	Yes	Yes
Edit Report Comments (CA View only)	No	Yes	Yes	Yes
View Report Information (Report metadata)	No	Yes	Yes	Yes
Create Web Viewer Internal Favorites (Report, Report Search Filter, Cross-Report Search Filter, Cross-Report Index-Value Filter, Cross-Report Index-Value Report Section, Report Index, and Report Index-Value Report Section)	No	Yes	Yes	Yes

View Web Viewer Internal Favorites (Report, Report Search Filter, Cross-Report Search Filter, Cross-Report Index-Value Filter, Report Index, and Report Index-Value Report Section)	No	Yes	Yes	Yes
Remove Internal Web Viewer Favorites (Any Type)	No	Yes	Yes	Yes
View Unsubscribed Material	No	Yes	Yes	Yes
View Annotations Notes (CA View only)	Yes	Yes	Yes	Yes
Other Annotation Actions (CA View only) (View Annotations, Edit Annotations, Delete Annotations, Create Annotations, Create Annotation Notes, Delete Annotation Notes, Create Annotation Bookmarks, View Annotation Bookmarks, Delete Annotation Bookmarks,	No	Yes	Yes	Yes
Subscriptions (Create Private Subscriptions, Create Public Subscriptions, Delete Your Subscriptions)	No	Yes	Yes	Yes
Assign Subscriptions to Roles	No	No	Partial, can only edit Roles below this Role in the hierarchy	Yes
View Role Hierarchy	No	No	Partial, can only see Roles below this role	
View, Edit, Delete Role Properties	No	No	Partial, can only edit Roles below this Role in the hierarchy.	Yes
Create New Role	No	No	Yes	Yes
Create Profiles	No	No	Yes	Yes
Assign LDAP Directory to Repository	No	No	Partial, can only edit Roles below this Role	Yes

Profile (View Edit, and Delete)	No	No	Partial, can only access users created by this Role or sub Role of this Role	Yes
User (Create, Edit, Delete, and Find)	No	No	Partial can only access users created by this Role or sub Role of this Role	Yes
Repository (Create, edit properties, or delete)	No	No	No	Yes
Create LDAP Directory Reference	No	No	No	Yes
Edit System-wide Preferences	No	No	No	Yes
View Repository Status Panel	No	No	No	Yes
View User Status Panel	No	No	No	Yes
View Admin Information Panel	No	No	No	Yes
View Audit Log	No	No	No	Yes
Import Admin Objects	No	No	No	Yes
Export Admin Objects	No	No	No	Yes

How CA OM Web Viewer Uses Roles

You can separate administration into a hierarchy of Group Administrator Roles, so that each Administrator is responsible for a subset Administration.

For example, report administration can be separated into two regions, with a Group Administrator for the West Region, and a Group Administrator for the East Region. For example, if there are three branches in the East region, the administrator might further split up report administration by branch--and create three additional Group Administrators, one for each branch in the region.

Each regional Group Administrator role would have read/write access to all branch-level Group Administrator roles, and would also have read/write access to all the roles created by the branch-level Group Administrators.

How Role Hierarchies Work

The System Administrator role object has full system permissions and can create all role types in the system. You can create roles of any type, other than System Administrator. Only System Administrator or Group Administrator role types can create new Roles.

Note: If you log in as a Group Administrator, you can create a Basic User, Advanced User, or another Group Administrator. However, you cannot create a System Administrator. You can only create a role with equal or lesser permissions than your current logged-in role.

Important! You can assign more than one User ID to the System Administrator, but the system only permits one role object of this type.

Consider the following information:

- All roles that you create can only have the permissions of the parent role, or more limited permissions.

  For example, if your role can print, you can assign printing privileges to a role that you create.

- By default, all roles that you create are subroles to your current role. If you create a subrole for a role that you are not currently logged in as, use the create subrole option.

  Note: A subrole descends from another role directly. A subrole can never have more permissions than the role above it in the hierarchy. All roles are a subrole of some other role, except the System Administrator; the top role in the hierarchy.

- Each role object has a type, and each type has a specific set of permissions.

- Parent roles can create other roles, and they always have the full permissions of the child role objects that they create.

  For example, the System Administrator creates a Group Administrator. The Group Administrator creates an Advanced User. The parent System Administrator has all the permissions of the Advanced User child object.

- Although you can create different roles with different privileges, each role must be one of the three basic types: Group Administrator, Advanced User, or Basic User.

- Each role type has access to a different set of core functionalities.

  Note: Role or repository settings can further limit these functions.

- System or Group Administrators can provide an extra role description on the Role tab. This additional information can help further clarify the purpose of a role. Only System Administrators and Group Administrators can view the role descriptions.

- If you remove a role privilege or repository, that privilege or repository is removed from all roles under the role in the hierarchy automatically.

- Adding a repository or privilege to a role does *not* mean that privilege or role adds to its subroles.

Note: The hierarchy of roles appears like a tree. Each subrole can only have access to privileges less than or equal to the role above it in the tree.

- One possible exception to the permission hierarchy is created by assigning a user to a role. You can assign a user to a role regardless of whether you assigned that user to the parent role.

Role Hierarchy Example

You can separate administrators into a hierarchy of Group Administrator roles, so that each Administrator is responsible for a subset administration. For example, assume that your sales for a specific state are divided into Eastern and Western counties. The Eastern counties further divide into four regions, and Western counties divide into two regions:

- Administration can be sectioned into two divisions, with a Group Administrator for East, and a Group Administrator for West.
- The Eastern Group Administrator further splits report administrators to an extra four regional Group Administrators; one for each region in the Eastern division, while the Western Group Administrator used similar segmenting for their two regions.
  - The Eastern Report Administrator Role would have read/write access to all four region-level Group Administrator Roles.
  - The Western Report Administrator Role would have read/write access to the two region-level Group Administrator Roles.
- Both Administrators would have read write access to all the Roles created by their region-level Group Administrators.

Note: Roles that are based on a higher role in the hierarchy are referred to as *lower* or *subroles* throughout the documentation.

Understanding Role Types

Role *types* are role permission objects that can be created and updated as required.

Although you can have as many different Roles as you need, there are only four different Role types. Each Role type has access to a different set of core functions. The Role types are:

- System Administrator

  The System Administrator type can change any CA OM Web Viewer setting and has total access to the Web Viewer system. This role can assign any privileges to any Roles or users.

Although most Roles allow you to have more than one Role object in a particular type, you can only have one System Administrator Role object, *System Admin.* However, you can add more than one User to this Role to have more than one person with System Administrator privileges.

Note: Be aware that being a System Administrator does not let you circumvent existing data access controls and security in CA View, CA Dispatch, and CA Bundl.

- Group Administrator

  The Group Administrator type is designed to be used to delegate the work required for report administration. The Group Administrator Role can only assign data that has been assigned to it by a System Administrator.

  You can divide your report administration into smaller groups, then further divide those groups into several others, designating other Group Administrators as needed. The Group Administrator Role for the smaller group would only have access to the Repositories and privileges that the Role above it assigned to it.

  Note: Group Administrators do not have the ability to add Repositories or LDAP Directories to CA OM Web Viewer or access system wide properties.

- Advanced User

  The Advanced User Role type lets users do the following:

  - Search Repositories for specific Reports and Cross Report Indexes
  - Create Favorites
  - Create Subscriptions in the repositories their role has access to.

  Although these users can create Subscriptions, they cannot assign Subscriptions to other users and have no control over the settings and permissions of other users.

  Note: This Role type has privileges similar to the users of CA OM Web Viewer 11.x.

- Basic User

  The Basic User Role type is the most restricted. These Roles cannot actively search for report content. The content these Roles can access is assigned to them by a Group Administrator or a System Administrator in the Role with the privileges to edit that Basic User Role.

Note: For more information about what each role type can be setup to use, see the Role Type Chart (see page 26).

View the Roles in Your System

To display all of the roles which you have access, select the Role subtab from the Administration tab. System Administrators can view all roles in CA OM Web Viewer. Group Administrators can view all roles that the current role created. If the Group Administrator creates other Group Administrator roles, the top-level Group Administrator can access all the roles that the lower Group Administrators created.

Follow these steps:

1. From the Administration tab, click the Role subtab.
2. (Optional) Click the plus or minus symbol next to a Role to show or hide the sub Roles of that Role.
3. (Optional) Click refresh to refresh this list from the database.
4. Click Role and view its settings and parameters.

Create a Role

A role can only have the permissions of the role of the parent. For example, if your role can print, you can assign printing privileges to a role that you create. Any role that you create is a subrole of your current role.

Follow these steps:

1. From the Administration tab, click the Role subtab.
2. Click Create Link.
3. Enter a role name, such as Bank Teller.
4. Select a role type, such as Basic User.

   Optionally, from this panel you can:

   - Set up role settings.
   - Select how users in this Role are authenticated.
5. Click Create.

   The Role is created.

Create a Subrole

A subrole is a role that is based on another Role. You can only assign permissions to the new role that are equal to or less than the Role you are basing the new Role on. For example, you want to create a subrole for the *Sales* role named *Sales Eastern*. This subrole can only have permissions less than or equal to *Sales*. To set up a subrole, you select the parent role and create a subrole for it.

Follow these steps:

1. From the Administration tab, click the Role subtab.
2. Select a role from the list.

   Important! The role that you create cannot have permissions greater than this role.
3. Click Create Sub Link and view the Create Role panel.
4. Enter a role name, such as Bank Teller.
5. Select a role type, such as Basic User.
6. Optionally, from this panel you can:
   - Set up any Role settings (See Editing Roles Settings)
   - Select how users in this Role are authenticated (See Role Authentication)
7. Click Create.

   The Role is created.

Edit Role Properties

You can edit role properties if the role is a sub role of your current role. Additionally, you can edit any role below your role in the hierarchy.

Note: Certain properties maybe grayed out, and you cannot change them. These properties might be inherited from the role above this role in the hierarchy. Also, you cannot change a role from Group Admin to another type when the role has sub roles.

Follow these steps:

1. From the Administration tab, click the Role subtab.
2. Select a role from the list in the left pane.
3. Choose one of the following tabs:

   Definition

   Specify a name, type, description, and authentication method, auto-enrollment setting, and set the repositories that this role can access.

   Properties

   Set Report Actions and Favorites capabilities

   Subscriptions

   Specify the subscriptions that are available to this role.

Role Authentication

CA OM Web Viewer users can authenticate with LDAP, External Security EXIT, or Mainframe Security. Advanced User type roles can authenticate with either mainframe security or LDAP security using the LDAP Mainframe Hybrid Profile Object. The Basic User can authenticate with three methods, depending on role settings. However, all other role types require Mainframe Security.

Consider the following information about authenticating roles:

- The Edit Role panel controls the authentication method of the role.
- You must select a Role Type of Basic User or Advanced User to change a Role authentication method from the default authentication method, which is mainframe authentication.
- If you select LDAP authentication with a Role Type of Basic User, supply both LDAP information and a profile (proxy mainframe account) for the role.
- If you select LDAP authentication with a Role Type of Advanced User, you must supply both LDAP information and the built in LDAP Mainframe Hybrid Profile Object
- Only Roles with a Role type of Basic User or Advanced User can use LDAP authentication.
- You can use automatic enrollment with an LDAP authenticated role.
- If you select External Security EXIT authentication, you must select Non-Mainframe users with a predefined profile named EXIT and a predefined directory name EXIT.
- Automatic enrollment is selected from the role panel for any roles defined with External Security EXIT authentication.
- You do not have to select automatic enrollment from the role panel for mainframe automatic enrollment.

  Mainframe automatic enrollment places mainframe security authenticated users into the role named Default User.

Profile

A Profile is an object that is used to provide the LDAP users with a mainframe password.

These objects are primarily a set of mainframe credentials sent to the mainframe when an LDAP authenticated user wants to perform an action on the mainframe.

Notes:

- The LDAP Mainframe Hybrid Profile Object sends the LDAP credentials of a user to the mainframe rather than a separate set of credentials.
- The EXIT Profile Object sends the mainframe credentials that are returned from exit calls to the mainframe rather than a separate set of credentials that are stored within Web Viewer.

LDAP Directory

An LDAP Directory is used to provide information about your LDAP sever and the attributes needed to authenticate a user.

Notes:

When setting up a Role you use a predefined LDAP Directory which also can be used with Auto Enrollment.

When setting up a Role with External Security EXIT authentication, you have to use a predefined EXIT Directory which is used with Auto Enrollment.

Auto Enrollment

The Automatic Enrollment check controls whether you want this Role to automatically enroll a member of a certain LDAP or external user directory. Basically, anyone who authenticated through this directory is added to this Role.

Note: You cannot auto enroll the members of a directory into two different Roles.

Setting the Role Authentication Method

To change the authentication method for a role, you must have a System Administrator or Group Administrator role type. Otherwise, you must use mainframe security.

Note: A role cannot have any sub roles if you want to change its type to Basic User.

Follow these steps:

1. From the Administration Tab, click the Role subtab.
2. Select a role from the list
3. Click the Definition tab in the edit panel.

4. Select a role type of Basic User

   Notes:

   - Only roles with a role type of Basic User or Advanced User can use LDAP authentication.
   - Additionally, roles with a type of Advanced User can only use the LDAP Mainframe Hybrid Profile Object when using LDAP authentication.
   - If a role has subroles, you cannot change the type of the role to Basic User. You must first delete the subroles of a Group Administrator type role before changing its role type.

5. Find the Role Profiles section and select the Non-Mainframe Users with a Profile option.

   If you want the LDAP credentials of the user as the same as mainframe credentials to be sent to the mainframe, select the LDAP Profile, which is the LDAP Mainframe Hybrid Profile Object. Otherwise, select a different Profile, which specifies which credentials should be sent to the mainframe.

   Note: With External Security EXIT authentication, a predefined Profile object and Directory object, EXIT is automatically selected for Non-Mainframe users.

6. Select a Profile from the first drop-down list on the right.

   If no alternate Profiles are listed, you must first create a Profile from the Profile tab.

7. Do *one* of the following:

   - Select an LDAP Directory from the next drop-down to the right.

     If no LDAP Directories exist, you either create a new Directory or enter the attributes listed below.

   - Manually enter the LDAP attributes needed to authenticate the users of the role.

     Enter values for LDAP Server, LDAP Port, Login Attribute, and Base DN.

     For more information, see User Authentication - Directory Settings and their Meanings

     Notes:

     - It is important to be aware that these options are overwritten when selecting a new LDAP directory.
     - If you want to permanently retain these options, we suggest that you have a member of the System Admin role create an LDAP Directory object. The LDAP Directory objects are retained permanently.

8. (Optional) Click the Automatic Enrollment checkbox.

   With the Automatic Enrollment option selected, any LDAP users that are authenticated with the selected LDAP setup are placed into this role automatically.

9. Click the Update button near the top right of the panel.

   The authentication parameters are saved.

Customizing Role Settings

The role determines the types of privileges that are granted to a user. Only System or Group Administrators can customize roles. You can only customize Roles below your current Role in the Role hierarchy.

Follow these steps:

1. From the Administration Tab, click the Role subtab.
2. Select a Role from the list.
3. Choose one of the following tabs:

   Definition

   Specify a name, type, description, and authentication method, and specify the repositories that this role can access.

   Properties

   Set the capabilities for Report Actions and Favorites.

   Subscriptions

   Specify the subscriptions that this Role can access.

Assigning Repositories to Roles - Overview

There may be situations where only certain repositories need to be available to a Role. Depending on how your reports are divided among your Repositories, you may want to only allow a Role to access a single Repository.

For example, if all your Sales Reports are in a certain repository, the Salesman Role would be allowed access to that repository, but might not be allowed to access a repository that contains accounting information.

The Repositories that can be assigned to a Role must be accessible by and assigned to the parent Role. For more information, see the Example of how to Use Role Hierarchy topic..

Notes:

- A repository maps to exactly one CA View, CA Bundle or CA Dispatch system. (See Repository Object for more information.)
- From this screen you cannot edit the Systems Administrator Role. Therefore, to allow the Systems Administrator Role access to a Repository object, you must add the Systems Administrator Role to the Repository at the edit Repository panel.

For more information about adding a repository to the System Admin Role, see Editing Repository Objects - Owner Roles.

Add a Repository to a Role

With the exception of the System Administrator Role, use the following procedure to add or remove access to a Repository object for a particular Role.

Follow these steps:

1. From the Administration tab, click the Role subtab.
2. Select the Definition tab,
3. Locate the Repositories section

   There are two lists Available Repositories and Selected Repositories.

   The Available Repositories List includes all the repositories you are allowed to assign to the Role. The Available list includes all the Repositories assigned to the Role directly above this Role in the Role hierarchy.
4. Select one or more repositories in the Available Repositories list.

   Hold Ctrl or Shift while clicking to select more than one repository
5. Do *one* of the following:
   - Click the single right arrow between the two lists to add the selected repositories.
   - Click the double right arrow to add all the repositories to the role.
6. Click Update in the top right corner of the pane.

Remove Repositories from a Role

Do the following to remove access to a Repository from a Role:

1. Click the Administration tab.
2. Click the Role subtab.
3. Select a Role from the Role list.
4. Click the Definition tab.
5. Locate the Repositories section.

   Two lists are displayed, Available Repositories and Selected Repositories.
6. Select one or more repositories in the Selected Repositories list.

   Hold Ctrl or Shift while clicking to select more than one repository
7. Do one of the following:
   - Click the single left arrow between the two lists to remove the selected repositories.
   - (Optional) Click the double left arrow to remove all the repositories from the Role.
8. Click the Update button near the top right corner of the panel.

   The targeted repositories are removed and the Role is updated.

Assigning Users to Roles

The Members section of the Definition tab lets you specify which users have the privileges associated with the Role you have chosen.

Add Users to a Role

If a user is reassigned or promoted, you can simply move that user to a different existing Role. For example, a Bank Teller who has been promoted can be added to the Bank Manager Role.

Do the following to add a user to a Role:

1. From the Administration tab, click the Role subtab.
2. Select a Role from the Role list.
3. Select the Definition tab.
4. Find the "Members" section.

   Two lists are displayed, Available Users and Selected Users.

   The Available Users in the list are displayed as follows:

   - User objects created by the Group Administrator Role directly above the Role you are editing in the Role hierarchy.
   - User Objects that are members of the Role directly above the Role you are editing in the Role hierarchy
   - Your own User name

   Any of the Users can be added as a member to this Role.
5. Select one or more names in the Available Users list.

   Note: Hold Ctrl or Shift while clicking to select more than one user
6. Click the single right arrow between the two lists to add the selected users

   (Optional) Click the double right arrow to add all the users to the Role.
7. Click Update at the top right of the pane.

   Note: Additionally, if your Role has the right to edit a user, you can add and remove Roles from a single user from the User panel. For more information, see User - Member Of.

Remove Users from a Role

Follow these steps:

1. From the Administration tab, click the Role subtab.
2. Select a Role from the Role list.
3. Click the Definition tab.

   Find the Members section.
4. Select one or more names in the Selected Users list.

   Hold Ctrl or Shift while clicking to select more than one user
5. Click the single left arrow between the two lists to remove the selected users.
6. (Optional) Click the double left arrow to remove all the users from a Role.
7. Click the Update button at the top right corner of the panel.

Note: You can add and remove Roles from a single user from the User panel. (See User -Member Of)

Enable or Disable Report Actions

You can enable or disable various report actions such as Emailing, Printing, File Saving, and Exporting. However, you can only enable Report Actions which are enabled in the role above this one in the hierarchy.

Additionally, when you enable a report action such as printing, you can set a page limit. If you set the print page limit value to 1000, a user would only be allowed to print a maximum of 1000 pages at a time. Some roles do not need printing at all, or only print a few pages.

Follow these steps:

1. From the Administration tab, click the Role subtab.
2. Select the Properties Tab.
3. Find the Report Actions section.
4. Click the appropriate radio buttons to enable or disable the Report Actions for eMailing, File Saving, Printing, and Exporting for this role.
   - (Optional): For enabled Report Actions, enter a page limit. A limit of 0 pages means that no limit is applied.
5. For eMailing and File Saving you can set the Text Report Format for the file:
   - Keep as Text - The format is not changed.
   - Convert to PDF - Text reports are automatically converted to PDF reports.
   - User Choice (Text or PDF) - Allows the user to choose whether the text stays in the original format or is converted to PDF.
6. For eMailing, you can set the eMail Type if both types have been selected and configured (see Preferences > Output Defaults):
   - Client based MAPI
   - SMTP (web form)
   - User Choice (MAPI or SMTP)
7. Click Update to update the report actions.

Specifying Permission to Designate Favorite Reports

To create a subscription (a group of reports targeted for specific users) you must be able to designate a report as a "favorite".

Specify whether the Role you are defining is to have the Favorites feature enabled or disabled. Some Roles are only allowed to view subscriptions so the ability to create favorites is therefore turned off.

Follow these steps:

1. From the Administration tab, click the Roles subtab.
2. Select the Properties Tab.
3. Find the "Favorites" section and click:
   - Disable
   - Enable
4. Click the Update button at the top right corner of the pane.

   Favorites permissions are updated for this Role.

Report Subscriptions in Roles

One of the key features of CA OM Web Viewer is the subscription method of report access.

Favorite reports listed on the Reports tab are based in part on the subscriptions assigned to your Role. For Basic Users, all the reports they see are assigned to them in the form of subscriptions.

For more information, see Subscriptions.

Assign Subscriptions to a Role

Follow these steps:

1. Click the Administration tab.
2. From the edit Role panel, click the Role subtab.
3. Select a Role from the Role list.
4. Select the Subscription tab

   There are two lists "Available Subscriptions" and "Selected Subscriptions."

   The Available Subscriptions list includes three parts:

   - All public Subscriptions
   - All private Subscriptions created by users while logged in as your current Role
   - All private or public Subscriptions assigned to the Role directly above this Role in the Role hierarchy

   See Private vs. Public Subscriptions.
5. Select one of more subscriptions in the Available Subscription list.

   Hold Ctrl or Shift while clicking to select more than one subscription.
6. Do one of the following:

   - Click the single right arrow between the two lists to add one or more selected subscriptions.
   - Click the double right arrow to add all the subscriptions to the Role.
7. Click the Update button at the top right of the pane.

Remove Subscriptions from a Role

Follow these steps:

1. Click the Administration tab.
2. From the edit Role panel, click the Role subtab.
3. Select a Role from the Role list.
4. Select the Subscription tab

   There are two lists, Available Subscriptions and Selected Subscriptions.
5. Select one of more subscriptions in the Selected Subscription list.

   Hold Ctrl or Shift while clicking to select more than one subscription.
6. Do one of the following:
   - Click the single right arrow between the two lists to remove the selected subscription(s).
   - Click the double right arrow to remove all the subscriptions from the Role.
7. Click the Update button near the top right of the panel.

   The Role is updated.

Managing User Authentication

You can set up the authentication methods that your users require. Auto enrollment options place users in roles automatically. CA OM Web Viewer uses the following authentication methods:

LDAP

Let users view mainframe reports without having mainframe set up credentials for those users.

Note: With LDAP authentication you can enroll users into Roles based on their LDAP attributes.

External security EXIT

Uses Java programming interface as exit calls to external authentication functions (customer supplied) to authenticate domain/network users for mainframe report access. This is an integration solution to customer existing Single-Sign-On system.

Mainframe security

Uses CA Top Secret, CA ACF2, or RACF authentication. There is a default user role that mainframe users can be enrolled into.

Note: Different users on the same Web Viewer system can be authenticated with different LDAP and Mainframe security methods.

Mainframe Authentication

Mainframe authentication refers to your mainframe security system. This type of security requires CA Top Secret, CA ACF2, or RACF authentication to gain access to CA OM Web Viewer.

The mainframe username must match the defined User ID in CA OM Web Viewer. The mainframe username is your mainframe username on the same LPAR as the DRAS used for security check.

Note: Any user that mainframe security verifies, but does not have a user account set up in CA OM Web Viewer is automatically enrolled with access to the Default User Role.

CA Output Management Web Viewer Single Sign On

Users are not required to log in to each repository separately. Users only provide their credentials when logging in to CA OM Web Viewer.

We recommend that all CA View, CA Dispatch, and CA Bundl repositories either use external security, or that you synchronize the credentials in some other manner.

If your repositories do not have synchronized passwords, each user must configure separate passwords for each repository object. Use the credentials section of the Configuration tab.

Auto Enrollment Mainframe Users

By default for the initial login, CA OM Web Viewer creates a user object and places a mainframe-authenticated user in the Default User Role.

- Any user with valid mainframe security credentials can log in to the product.
- The Default User Role has been set up for mainframe-authenticated users.
- After the user logs in, the system places the user in the Default User Role automatically. You can edit the options for this role, just as any other Role.
- You can give the role access permissions that range from none to all repositories.
- Existing security definitions that the base mainframe repositories defined are not bypassed, and can be used to limit access for users.

Note: If you enable LDAP security before mainframe external security, some users may not enroll automatically. LDAP would authenticate these users first, and then place the users into the LDAP Role, and not auto-enroll mainframe users.

LDAP Authentication

LDAP authentication lets you bring large numbers of nonmainframe users to view report data without your having to define all the users to your mainframe security system and/or to each CA View and CA Bundl repository.

Requirements

- Only Basic User type roles can use LDAP authentication

  Note: One exception is the LDAP Mainframe Hybrid Profile Object, which lets the LDAP credentials of a user to be the same as mainframe credentials to be passed to mainframe security.

- Users that authenticated through LDAP can view data from CA View and CA Bundl repositories, but cannot access data from CA Dispatch repositories.

  Note: For other role types, users must be mainframe authenticated users.

Profiles

- You define a single user mainframe user account and create a shared profile in CA OM Web Viewer so that many LDAP users can use that single user mainframe account.

  This mainframe user ID is basically a trusted account that is used as a proxy user for all the users who share a Profile.

  Therefore, you can let your existing LDAP system authenticate the users who share the single set of credentials for the repositories and or for mainframe security.

- We recommend that all Profiles refer to a set of mainframe security credentials, rather than repository level internal security credentials. This practice simplifies administration and usage.

  For example, it would be confusing to have the profile credentials expire at different times for different repositories.

- You can define more than one Profile if necessary.

  For example, you can have a different Profile for each Role you authenticate through LDAP. Each Profile can have access to different material. From the mainframe it can appear that the same Profile user is logged on many times. The Profile user might have 200 logins listed if 200 LDAP users share that profile.

Directories

- A role has an assigned Directory object so that members of that role can be authenticated using LDAP.

  Because the Basic User type Role can have an assigned Directory object, members of that Role can be authenticated using LDAP.

- Directories contain information which can be used to authentic users to CA Output Management Web Viewer.

- Only a System Administrator can create a Directory object, and this object defines:

- The LDAP server and port
- LDAP Base DN and password
- LDAP Login attribute.

- If you do not want a user to use a Directory object, you can manually enter LDAP attributes into a role. LDAP bind settings are only available by creating a Directory object at Directory panel.

Auto Enrollment LDAP Users

LDAP authentication lets you add users to a particular role automatically. Auto Enrollment is similar to standard LDAP authentication because it also requires an association between a directory object and a particular role.

A role that uses LDAP authentication can allow or not allow auto-enrollment:

- With auto-enrollment turned on in the same role, any user authenticated with the Directory referenced by the role is added to that role. CA OM Web Viewer creates a user object if needed.
- Without auto-enrollment, even if a user passes LDAP authentication, the user is not added to the role. Only existing users of that role can log in.

  User objects can be manually created from the user panel and added to the role manually.

Note: You must set up auto-enrollment in the edit roll panel.

Auto Enrollment Considerations

- We suggest that you only attempt to auto enroll a single user into a single role.
- Users can only be auto-enrolled into a single role, unless the user uses a separate password for each role, and each role has a separate Directory set up.
- If the user is a member of an LDAP-authenticated role, do not use automatic enrollment to enroll them into another role
- It is an administration error to have a user in more than one role authenticated by different LDAP setups which share credentials.

  Your user can only log in as Role A or Role B, and you cannot determine ahead of time which role they are logged into by CA OM Web Viewer.
- Normally, CA OM Web Viewer performs the following steps:
  - Find the first LDAP role the user is eligible for with the supported credentials
  - Log the user in to that role, automatically enrolling them if necessary

    Remember that CA OM Web Viewer does not continue to check to see if the user is eligible for other roles.
- If you check mainframe security before LDAP security, some of your users might not be automatically enrolled. (See Preferred Security System Order).

  The following situations might occur if the LDAP and mainframe credentials of a user match and you check mainframe security before LDAP security.
  - Your user might be auto-enrolled into the Default User Role with the mainframe credentials if the mainframe credentials are the same as the LDAP credentials.
  - Additionally, the user might be logged into a different role that uses mainframe credentials for authentication.

LDAP User Generation

When a user enrolls in a role automatically, and if the user does not exist, CA OM Web Viewer creates a user object. The new User object has several of its fields auto-populated from your LDAP directory. For this auto population to occur, your LDAP system must support this kind of lookup, and use the appropriate naming conventions.

Note: Only newly created users have their attributes populated, existing users are not modified even if they are automatically enrolled in a role.

The following LDAP attributes automatically map to the equivalent values in the CA OM Web Viewer User object.

LDAP Attributes Automatically Imported	Web Viewer Mapping
Administrator supplied Login Attribute, defined at creation of a Directory object or from the Role profile section of the edit/create Role panel.	User ID
givenName	First Name
sn	Last Name
title	Title

For more information about the User object fields, see Editing User Objects in the User section.

External Security EXIT

The External Security EXIT uses Java programming interface as exit calls to external authentication functions (customer supplied) to authenticate domain/network users for mainframe report access. This is an integration solution to the customer existing Single-Sign-On system.

Security System Checking Order for Mainframe and LDAP Authentications

Depending on your installation settings, CA OM Web Viewer checks your LDAP or security credentials first. You normally configure this setting during installation on the LDAP Host Information panel.

Note: For more information about indicating LDAP user authentication, see the *Installation Guide*.

Regardless of the order of the security checks, if the user fails the first type of security check, the second type of security check is called.

For example, if the LDAP security is checked first and the user failed all of the LDAP Directory checks, CA OM Web Viewer attempts to check user credentials against mainframe security next.

Be aware that this setting might also affect your auto enrollment options.

- With mainframe security checked first, if your user passes the mainframe security check, that user logs in to CA OM Web Viewer, and never checked against the LDAP system or enrolled into the Role using LDAP authentication.
- With LDAP security checked first, the user is logged in to CA OM Web Viewer before they are given a chance to be automatically enrolled in the Default Role by mainframe security.

If your user has separate credentials for LDAP and mainframe security, this issue does not occur. It is only an issue when the user name and password are the same for both types of security.

External Security EXIT Authentication

External Security EXIT authentication refers to your existing Single-Sign-On security system external to Web Viewer. This authentication method is an extended Web Viewer LDAP security model via exit calls to determine the user access. This lets you bring large numbers of domain users to view report data without your having to define a mainframe profile and a LDAP directory system within Web Viewer.

A predefined profile object is called as EXIT with all profile fields set to EXTERNAL associated with a predefined Directory object named EXIT with all LDAP fields set to EXTERNAL. That means the user proxy profile and user LDAP directory systems are all external to Web Viewer and rely on External Security Service EXIT calls to authenticate web login users using external user directory system and obtain the mainframe user ID for the web user if validated.

Requirements

- Except System Administrator, other user type roles can use External Security EXIT authentication

  Note: The System Administrator must use the CA Output Management Web Viewer login form with mainframe credentials to log in to the System Administrator role.

- Users that authenticated through External Security EXIT and assigned a shared mainframe profile can view data from CA View and CA Bundl repositories, but cannot access data from CA Dispatch repositories (CA Dispatch does not allow for shared credentials).

Profile

- EXIT Profile presents a mainframe profile with credentials not stored in Web Viewer, but in customer SSO security system.
- You can define a single mainframe user account as EXIT profile returned from exit calls to map your users to a mainframe profile so that many web users can use that single user mainframe account for mainframe report access.

  Therefore, you can let your existing SSO security system authenticate the users who share the single set of credentials for the repositories and or for mainframe security.

- We recommend that EXIT profile refers to a set of mainframe security credentials returned from exit calls rather than repository level internal security credentials. This practice simplifies administration and usage.

  For example, it would be confusing to have the profile credentials expire at different times for different repositories.

Directory

- EXIT Directory contains information which is all external to Web Viewer with all LDAP fields set to EXTERNAL.

- A role has an assigned EXIT Directory object so that members of that role can be authenticated using authentication exit calls.

Auto Enrollment External Security EXIT Users

By default for the initial login, CA OM Web Viewer creates a user object with the web login user ID and places the authenticated user in the EXIT User Role automatically.

- Any user validated via exit calls can log in to the product.
- The EXIT User Role has been set up by System Administrator for Exit-authenticated users.
- After the user logs in, the system places the user in EXIT User Role automatically. You can edit the options for this role, just as any other Role.
- You can give the role access permissions that range from none to all repositories.

Managing Profile Objects

Profile objects let multiple LDAP users log on to CA View or CA Bundl with an alternate mainframe user account. You can create a standard profile object or an LDAP mainframe hybrid profile object.

Normally, a profile maps multiple LDAP users to a single mainframe account. However, the build in the LDAP mainframe hybrid profile lets each user authenticate through LDAP. The user can then use the LDAP passwords as mainframe passwords.

Note: If you delete a profile, a message indicates that the profile was successfully deleted. If the message indicates that the profile was not deleted, there are roles still assigned to the profile.

Standard Profile

The standard profile object provides a proxy set of mainframe credentials that all LDAP users share in a particular role. All LDAP users must have an assigned profile for their role, which determines their access to CA View or CA Bundl repositories. These credentials include either mainframe security credentials or internal security credentials for the various CA View or CA Bundl repositories.

Note: We recommend that all profiles use mainframe security credentials. Otherwise, verify the validity of the profile credentials for each CA View and CA Bundl system.

Profile Access

- Role access is limited to material its profile credential have access to on the CA View and CA Bundl systems.
- Role or repository settings can further limit access and permissions of users.

- If a user has access to data on specific repositories, the users can only gain access to the data of their role profile credentials.
- The standard profile uses a single set of mainframe credentials. All users that use this profile have certain limits on their actions, no matter which role uses the profile.

  Note: Administrators must be aware that the credentials supplied by a profile can expire in a mainframe security package. If they expire, a user from a similar role (or the System Administrator) must update the credentials.

  When assigning a subscription to a role which uses a profile, verify that the reports in the subscription are accessible by the profile and role. It may be confusing to assign subscriptions of reports from various repositories when the profile cannot access some of the repositories.

LDAP Mainframe Hybrid Profile

CA OM Web Viewer creates the LDAP profile automatically. This built-in profile does not supply a single mainframe credential for all the users in the profile; instead, it uses the LDAP credentials supplied by each individual user.

Consider the following information:

- Use this profile with caution, because it requires that the LDAP and mainframe credentials of a user are synchronized.
- This profile is named LDAP and CA OM Web Viewer creates this profile automatically. This built-in profile does not supply a single mainframe credential for all the users in the profile. Instead, it uses the LDAP credentials that each individual user supplies.
- If you delete this profile, you can recreate it by creating a profile named LDAP. Use *LDAP* for the user name and password.

  For example, a user logs in to LDAP with the following credentials:

  User: user1

  Password: pwd1

  CA OM Web Viewer sends these credentials to the mainframe.

Creating a New Profile Object

If you create a profile object while logged in to a "Group Admin" type role, members of that same role can assign the created profile to roles. Additionally, members of the System Administrator role can also assign any profile to various roles.

Follow these steps:

1. From the Administration Tab, click the Profile subtab.

   Click Create.

2. Enter a Profile Name.
3. Enter a User ID and Password.

   The User ID and Password are the values found in the credentials that send to CA View, CA Bundl, or external security when LDAP users are trying to access mainframe resources.

4. (Optional) Enter a Description

   This value is displayed on this panel, and also as a tool tip in the profile selection drop-down when an administrator is selecting this profile for a role.

   This field can be used to display information about the intended usage of this profile, or for notes to others who use or edit this profile.

   Notes:

   - The Assigned Roles field is read only and cannot be changed.
   - To add this profile to a role you must edit the role.
   - The Last Modification field is blank when CA OM Web Viewer creates the role.

5. Click Create.

Listing Profile Objects

The list of Profile objects you see depends on the Role you are currently logged in as:

- The System Administrator Role has access to all Profiles.
- The Group Administrator type Roles only have access to the Profiles created by that Role.

Follow these steps to view a list of Profiles:

1. From the Administration Tab, click the Profile sub tab.

   The Profiles list is displayed in the left pane.

   Based on your current Role, only the Profiles that you have the authority to modify are listed.

2. If there are more Profiles than can be listed on one page, use the navigation arrows to display other Profiles.

   >> displays the last group of Profiles

   > displays the next group of Profiles

   < displays the previous group of Profiles

   << displays the first group of Profiles

3. (Optional) Click the refresh button,  , to refresh this list from the CA OM Web Viewer database.

Profile Security and Auditing

Since a profile lets many users share a single set of mainframe security credentials, use extra care when you define the access to CA View or CA Bundl by these credentials.

Note: This section refers to using a profile a proxy user account, and is largely not applicable to the LDAP Mainframe Hybrid Profile Object.

Determining Access

- To determine profile access, view which roles have this profile. The Assigned Roles drop-down on the Edit Profile pane lists these roles.
- Anyone that successfully logs in to one of the Assigned Roles can access this profile.
- Depending on the role permissions, users may not have complete access to all the information in which a profile has access. However, a role that uses a particular profile can never have access to more information than the profile.

Disseminating Information

- All repositories or data assigned to a profile's credentials for CA View or CA Bundl can be assigned to any Basic User type role by the System Administrator or the Group Administrator who created the profile object.
- Members of the role who created the profile object are responsible for assigning it to the correct roles and users.
- Anyone in the same role as a profile creator can grant the right to grant the Profile to other Roles.
- Additionally, the System Administrator can assign the profile to any role.
- Once you give a profile access to information (Repositories or Reports), members of the Group Administrator role that created the profile or the System Administrator can assign any of the information that profile has access to any Basic User type role they have access to edit.

Auditing User Access

- CA OM Web Viewer lets you audit the actions of all users, and does not treat all users in a single profile as a single user.
- Although to CA View or CA Bundl auditing, all the LDAP users logged in to a single profile appear to be the same user logged in multiple times, in CA OM Web Viewer auditing they are audited separately.

  For example, if User A and User B both share a profile, their actions are audited separately in CA OM Web Viewer, but might appear like the same user logged in twice to CA View or CA Bundl auditing since they are using the same credentials as provided by the profile.

Managing User Objects

User objects are assigned to roles and derived from roles. You can change the properties of many users at once by changing a property of the role the user is assigned to. If a user changes a job function at your company, you only have to change the role or roles; you do not have to change many different properties of that particular user.

The users you are currently allowed to view and edit depends on your current Role. The System Administrator can view and edit any user on the system. If your current Role is a Group Administrator Role, you can only view and edit the users created by your role or sub role of your role.

User Object Properties

Use this object to define your users. Several fields on this pane are optional and are used to provide reference and administration information. Some of the optional fields only appear on this User pane.

Note: User ID, first name, last name, title, and description can be automatically filled with the user attributes from an LDAP user directory. Your LDAP system must permit a lookup of this type and use a compatible attribute naming convention.

User IDs

You must assign a User ID to each user that matches their mainframe User ID, LDAP user name, or both. The exception is the LDAP Mainframe Hybrid Profile Object, which requires user ID to be eight characters or less, because the LDAP credential passes to the mainframe.

- If you want authentication for this User ID with an LDAP server, the User ID must match the LDAP user name.
- If user authentication is based on the mainframe User ID and password, the CA OM Web Viewer User ID must match the mainframe User ID.

Notes:

- If this User ID is going to be used to access the mainframe, it must have 8 characters or less.
- If this user is to be authenticated through LDAP, the User ID can be longer than 8 characters.

  With other LDAP configurations, the Profile associated with the role of this user must have a mainframe user ID that has 8 characters or less.

First Name (Optional)

- When user selection is involved, on some panes the optional first name and last name are displayed with the User ID.
- In some cases, the field can be automatically filled as part of the LDAP automatic enrollment process. For more information, see LDAP User Generation.

Last Name (Optional)

- When user selection is involved, on some panes the optional first name and last name are displayed with the User ID.
- In some cases, the field can be automatically filled, as part of the LDAP automatic enrollment process. For more information, see LDAP User Generation.

Title (Optional)

- This information only appears on this pane. For more information, see LDAP User Generation.

- In some cases, the field can be automatically filled as part of the LDAP automatic enrollment process.

Description (Optional)

- This information only appears on this pane.
- This optional field is used to add information about this user. Enter department information or details about the Roles an administrator can add to this user.

Member of (Optional)

The selected column of the Members Of section lists all the Roles that this user can access in CA OM Web Viewer. A Role provides permissions to access Repositories and the ability to perform certain actions.

Adding Roles to a User Object is optional, however, the user needs a Role to gain access to anything in CA OM Web Viewer.

Note: When using automatic enrollment, a Role can be automatically added to a user.

For more information, see Auto Enrollment LDAP Users or Auto Enrollment Mainframe Users.

Creating a New User Object

Follow these steps to add a User ID, optional values, and one or more Roles to the User Object:

1. From the Administration Tab, click the User subtab.
2. Click the Create link at the top of the User list in the left pane.

   The User ID fields are displayed in the right pane.

   - Enter a User ID

     This ID must match the mainframe User ID, LDAP user name, or both. If the User ID is intended to be used for mainframe access, it should only be 8 characters long.

   - (Optional) Enter a First Name and Last Name.

     We recommend that you enter values in these fields for ease of identification. The first name and last name are displayed along with the User ID on panels when user selection is involved.

   - (Optional) Enter values in Title and Description.

     We recommend that you enter a Title as a reminder when assigning Roles to this ID.

3. Find the Member Of section.

   There are two lists, Available Roles and Selected Roles.

   The Roles in the Available Roles list were created by your current Role, or are Roles created by sub Roles of your Role.

   For more information, see Role Hierarchy.

4. (Optional) Select one or more Roles in the Available Roles list

   - Hold Ctrl or Shift while clicking to select more than one repository.
   - Click the single arrow to move one Role or the double arrow to move all the Roles into the Selected Roles list.

5. Click Update at top right of pane.

   The User object has been created and connected to the specified Roles.

Finding a User in the User List

The users you are currently allowed to view and edit depend on your current Role. As a System Administrator you will be able to view and edit any user on the system. If your current Role is a Group Administrator Role, you will only be able to view and edit the users created by your Role or sub Role of your Role.

Follow these steps to view the list of users and find a specific user:

1. From the Administration Tab, click the User subtab.
2. The User ID list appears in the left pane.
3. Do one of the following to display a user object.
   - Locate the User ID in the list (recommended).
     - Use the single navigation arrows to move to the next page or the double arrows to move to the end or beginning of the list.
     - Sort the User Object list alphabetically.

       Click the User ID column header to display the user objects in alphabetic order.
   - Use the Find text box at the top of the left pane:
     - Enter the User ID in the Find text box.

       You can use an asterisk "*," as a wildcard in your search term. Only the first matching value is displayed with wildcard or partial name searches.

       To find a different user, define more specific criteria.
     - Click the binoculars icon.

   The User object is located. You can click the object to display the Edit pane where you can view or edit the settings.

Managing Directory Objects

Directory objects contain LDAP information for validating a group of users with your current LDAP system. An LDAP directory validates a group of users for access to a role, or to auto enroll users into a role. You click the Directory subtab to view a list of the directory objects.

Only System Administrators can add or edit a directory object. However, Group Administrators can view the settings of a directory object, and can assign directory objects to roles.

Directory name

Represents the directory object and all of its settings. When a System Administrator or a Group Administrator adds a directory to a role, this name appears as an option.

LDAP Server

Specifies the hostname or IP address of your LDAP server.

LDAP Port

Specifies the port number for your LDAP server.

Login Attribute

Specifies the attribute in your LDAP directory that represents your users' user ID. Common examples are cn (common name) and uid.

Base DN (Distinguished Name)

These attributes must be added to a users' login attribute to produce the distinguished name you desire. For more information, see How the LDAP Distinguished Name is Determined.

Description

An optional field seen only on the Directory tab by the System Administrator, not shown elsewhere.

The Description field is seen at this panel, and is also a tooltip in the directory selection drop-down list, when an administrator is selecting this directory for a role. This field can be used to show information about the intended usage of this Directory, or notes to others who use or edit this profile.

Assign Roles

Specifies every role which uses this directory for its authentication. Consider the contents of this field before you delete this directory. Additionally, this field can provide information about which users are given access to which roles.

Create a Directory Object

Use a directory object to store LDAP information for validating your users.

Follow these steps:

1. From the Administration Tab, click the Directory subtab.
2. Click Create above the Directory list.

3. Use the information in the Directory Settings and Their Meanings table and enter values for the following:

   Directory name

   Represents this object, and all of its settings. When a System Administrator or a Group Administrator adds a directory to a role, this name appears as an option.

   LDAP Server

   Specifies the hostname or IP address of your LDAP server.

   LDAP Port

   Specifies the port number of your LDAP server.

   Login Attribute

   Specifies the attribute in your LDAP directory that represents the user ID of your users. Common examples are *cn* (common name) and *uid*.

   Base DN and password

   Specifies the attributes that you add to the login for users to produce the distinguished name that you want.

   Description

   (Optional) Shows information about the intended usage of this Directory, or notes to others who want to use or edit this Profile

   Assign Roles

   Every Role which uses this Directory for its authentication appears here. Consider the contents of this field before you delete this directory. Additionally, this field can provide information about which users are given access to which Roles.

4. Click Create.

LDAP Distinguished Name Setup and Usage

Some LDAP systems require a password protected bind in order to authenticate other users. If your LDAP server is setup this way, you can add an LDAP Bind DN in the directory panel. The LDAP Bind DN is the distinguished name of an account that can authenticate other users. The LDAP Bind DN should be a complete DN, including login attribute, username, and the appropriate base distinguished name.

The following example describes how CA OM Web Viewer determines and uses the Distinguished Name:

Determination of the LDAP Distinguished Name

Assume that a user with the user name "Jim" logs into Directory A which has the following setup:

Directory A:

- Login Attribute: "cn"
- Base DN: "ou=west,ou=sales,dc=your_company,dc=com"

The resulting Distinguished Name would be:

cn=Jim,ou=west,ou=sales,dc=your_company,dc=com

Mapping LDAP attributes to Roles

- You can create different Directory objects to refer to different parts of the organization.
- In the above example, everyone one who gets authenticated through Directory A would have to be in the "west" and "sales" organizational units (ou).
- Dc and ou are commonly used LDAP attributes; however, your LDAP system might use a different naming convention.
- You change the Base DN for different Directory objects. This allows you to map different existing units within your organization to different Roles with in CA OM Web Viewer.
- A Role can only refer to one Directory object. However, several different Roles can all use the same LDAP Directory for authentication.
- In some cases your organizational divisions within LDAP might be too large for a single Role, so you can have two Roles that both refer to the same Directory object.

  Reminder: Only one of the Roles that refer to the same Directory object should use auto enrollment, because users can normally only be automatically enrolled into a single Role.

Managing Subscriptions

Subscriptions let you bundle reports, report sections, or search filters designated as Favorites. System Admin, Group Administrators, and Advanced Users can create and manage subscriptions. At the most basic level, a System or Group Administrator can use a subscription to assign reports to users. These users can simply see a select list of the reports that they require to use.

With a subscription, you can provide report access to Basic Users who no longer have to monitor which repositories contain which reports. These users do not have to search a repository, or even know the report name to view their reports online. The Subscriptions panel displays a list of the subscriptions that you created personally.

Note: To see a list of all subscriptions that you can assign to a role, go to the Subscriptions tab of the Edit/Create Role panel.

Favorite

Specifies a report or filter bookmark that you want to have quick access to online. You can select and add most of the viewable or usable entities as favorites. All these types of data are frequently referred to as *reports*. Subscriptions can contain any of the favorite types (see page 68).

Subscription

Specifies a group of Favorites that has been given a name and description. Administrators and Advanced Users can use the subscription name to assign this bundle of reports to one or more Roles. Only Advanced Users and Administrators can create Subscriptions, and only Administrators can assign the Subscriptions to other Roles. Subscriptions can be either private or public.

The difference between private or public is who can assign a subscription to a role. Only a member of the same role as the creator of the subscription can assign a private subscription to one or more roles. Additionally, only Administrator type roles can assign these subscriptions. Any System Administrator or Group Administrator with the ability to edit the role can assign a public subscription to a role.

Favorite Types

CA OM Web Viewer includes seven different types of internal favorites, but only six of them can be included in a subscription.

Product Favorites	Description	Display
Report	The simplest type of favorite that refers an entire report.	Each report displays as a clickable icon. The icon used depends on the format of the report.

Report Search Filter	You can save a report filter. If you save a filter as a favorite, you can use that filter the next time you want to see all the reports that are selected by that filter. For example, the favorite filter A* specifies the last 25 days on repository nnn. Whenever you use this favorite, all the reports that start with the letter "A" that were added to Repository *nnn* in the last 25 days are selected.	The reports matching this filter at runtime are listed in a subfolder of the subscription. Each time a user logs in and expands the folder the search filter checks to find reports matching the filter. You can expand and collapse the folder as needed.
Cross-Report Search Filter	You cannot add this type of favorite to a subscription, and it is not listed on the favorites list of the subscription panel.	** Not applicable, because this type of favorite returns index names (not reports). So, this type of favorite cannot be added to a subscription.
Cross-Report Index-Value Filter	This filter returns all report sections that match this index and value pair. You can save the filter as a favorite. For example, assume that you have a Cross Report Index of "ACCOUNT" with a value of "12345678." This filter can produce five different report page ranges, or report sections, where the index matches the given value. These report sections can actually be from different reports, if an index and value is in more than one report. Those report sections appear in a sub folder of the subscription on the Reports tab.	The matching report sections are listed in a subfolder of the subscription on the Reports tab. Each report section listed in the subfolder appears as a text report with the text report icon. 
Cross-Report Index-Value Report Section	A single report section You can add a single Cross-Report Index Value match as a favorite. This report section appears to a user of the subscription, as a text report listed in your subscription.	This report section appears to a subscription user as a text report and appears with the text report icon. 
Report Index	You can add Report Indexes as favorites. This type of Favorite lets the user of the subscription select an index value, and then see the matching section of data from a report for that index value pair.	When a user selects this type of report, the user is prompted for one or more index value selections. After the user selects the index values, a report section is displayed. This type of index appears with the report index icon. 
Report Index-Value Report Section	A single report section You can add a single report index value as a Favorite.	This report section appears to a subscription user as a text report listed in the subscription. 

Favorite Properties

The favorite properties have a number of effects on how users see favorites in subscriptions. The favorite properties can be viewed from the edit favorite properties dialog. The description column of the table includes how each property affects the subscription table.

The following list describes the favorite properties:

Favorite Name

Specifies the name that is displayed in the subscription on the Reports tab.

Favorite Description

Specifies the tooltip that is displayed in the subscription on the Reports tab.

Favorite Type

Specifies one of the following favorite types:

Latest Report

- The actual report data the user sees can change over time.
- If new versions of the report exist, the favorite always points to the latest version.

Static Report

- Refers to one particular version of a report.
- The actual report data does not change over time.
- You cannot include static favorites in a subscription.

  Note: A reorganization of your mainframe repository can break this link. For example, merging or splitting repositories in CA View can cause these favorites to point to the wrong report.

Filter Settings

- Refers to saved search filter settings.
- Use this type of favorite to rerun a search later.
- You cannot add the Cross-Report Index filters to a subscription.

Last Modification

Refers to either the creation date of the favorite, or the last time a user modified it after its creation.

Attributes

Different favorite types list different attributes. The following table lists the various favorite types with their attributes:

Type of Favorite	Icon	Attribute
Report or Report Section Favorite (Dynamic)		Attributes section includes only the Report ID.
Report or Report Section Favorite (Static)		Attributes section includes only the Report ID.
Report Filter Favorites		Various Filter criteria used to create the filter.
Cross-Report Index-Value Filter Favorites		Various filter criteria used to create this filter, with the index name and value.
Report Index Favorites (Dynamic)		Attributes section includes only the Report ID.
Report Index Favorites (Static)		Attributes section includes the Report ID, and the create date and time of the report this favorite is referring to.
Non-Text Reports (Dynamic)		Attributes section includes only the Report ID.
Non-Text Reports (Static)		Attributes section includes the Report ID, and the create date and time of the report this favorite is referring to.

Edit Favorite Properties

You edit the properties of a favorite from a subscription panel. To use this procedure, enable the *Show advanced options drop-down in favorites list* in the Favorites List section of the Configuration panel. Alternatively, you can edit the properties of a favorite from a selected repository, from the Advanced Search Tab on the Favorite List subtab.

Follow these steps:

1. From the Subscription Tab, view the Subscriptions in the left pane. If there are more subscriptions than are visible, scroll through the list.
2. Click a subscription.

   The edit Subscription fields appear in the right pane.
3. Find the Action column in the Favorites list

   If this column is displayed there is a button labeled Action in each row of the Favorites table. If this column is not displayed, see note before step one.
4. Click the button in the row of the Favorite that you want to edit.

   A drop-down menu appears.

5. Click the Favorite Properties option.

   The Favorites Properties dialog appears.

6. Edit the Favorite Name.

   Enter the name of the favorite that the users see in the subscription on the Report tab, after you assign the subscription to the users.

7. Edit the Favorite Description.

   Enter the tool tip of the favorite that the users see in the Subscription on the Reports tab, after you assign the subscription to the users.

8. Click Ok to update the properties.

Create a Subscription Using Favorites

A Subscription is a bundle of one or more favorites (reports or other types of data) that have been grouped into a named collection. Once created, these Subscriptions can be assigned by Administrators or Advanced Users to other users or they can be kept for personal use. Only Advanced Users and Administrators can create and manage subscriptions.

Note: The new Subscription appears in the Subscriptions list in the Reports Tab pane. It may appear slightly different to different users. For more information, see Assign a Subscription to a Role - Overview.

Follow these steps to create a Subscription:

1. From the Subscription tab, click the Create link above the Subscription List in the left pane.

   The create subscription panel appears in the right pane.

2. Find the User Favorite List and be sure that you have at least one favorite report listed.

   Since subscriptions are built with favorite reports, there must be at least one favorite available to include in the subscription. If you don't have at least one favorite in your list you must first designate one or more reports as favorites.

   Note: For more information about creating and using various types of favorites, see the *User Guide*.

3. Enter a Subscription Name.

   This is the name administrators see when choosing subscriptions to add to a Role.

4. Enter a Subscription Description.

   On the reports tab, users of the subscription see this explanation of the subscription contents.

5. Select one of the following:

   - Private radio button
   - Public radio button

   (See Private vs. Public Subscriptions)

6. Select at least one favorite.

   From the User Favorites List, locate a favorite that you want to designate as part of the Subscription and click the checkbox in the left column.

   Note: For more information about creating and using various types of favorites, see the *User Guide*.

7. Click the Create button at the top right corner of the pane.

   The Subscription is created.

Add or Remove Favorites in a Subscription

Add or remove a Favorite from a subscription by checking or unchecking the leftmost checkbox in the Favorite's row.

Note: Cross Report index filter Favorites (which return index names instead of reports), cannot be added to a Subscription. This type of favorite does not appear in this User Favorite List. For more information, see the Types of Favorites Table.

Follow these steps:

1. From the Subscription Tab, find the Subscription list in the left pane.
2. Click on a Subscription.

   The edit Subscription panel appears in the right pane.
3. (Optional) Update the following as required:
   - Name
   - Description
   - Type

     Click the appropriate radio button to change the designation.

     Note: For a description of these settings, see Create a Subscription Using Favorites.
4. Do one of the following:
   - Click the checkbox on the right to add the Favorite to this Subscription.
   - Uncheck the box to remove the Favorite from this Subscription.
   - If all the Favorites in the Subscription are not displayed, use the navigation arrows to scroll through the list.

   Notes:

   - If the Subscription has been assigned to a certain Role, any newly selected Favorites in the Subscription appear in that Roles' users' Report Tabs the next time they log into CA OM Web Viewer.
   - You can optionally, change the display name or description of a Favorite. For more information see Edit Favorite Properties.
5. (Optional) Click on the name of a Favorite to display the report or apply the Favorite's filter. This action lets you see the information the Favorite is pointing to.
6. Click Update in the upper right corner of the pane.

   The Subscription is updated.

Delete a Subscription

Be careful when deleting Subscriptions. The deleted Subscription is removed from every Role that it is currently assigned to. If you only want to remove a Subscription from a Role, you must edit the Role.

Follow these steps to delete a Subscription:

1. From the Subscription Tab, find the Subscription list in the left pane.
2. Click on a Subscription.

   The edit Subscription panel appears in the right pane.
3. Click the Delete link above the Subscription list on the left pane.

   A delete confirmation dialog appears.
4. Confirm the action to complete the deletion.

Assign a Subscription to a Role - Overview

When creating and assigning Subscriptions, there are a number of access considerations that should be checked to insure the intended users have access to the data you are attempting to give them. This section discusses some things to consider when creating and assigning a Subscription to a Role.

You cannot actually assign Subscriptions to Roles from the Subscription panel. To assign a Subscription to a Role, you must go to the Administration tab, edit Role panel. (See Role - Assigning Subscriptions to a Role)

When a System or Group Administrator wants to select a Subscription to add to a Role, they see a list of Subscription names. (These names should be meaningful and relevant so that the administrator has accurate information about the contents of the Subscription.)

In some cases, you might assign material to users and the users cannot see the material. To avoid this situation, use the following process:

1. View the Subscription in your Reports Tab and check for any problems by viewing the Subscription yourself.

   Note: Newly created Subscriptions automatically appear in your own report list.

2. Assure Repository access.

   - You cannot give a user access to a Favorite if the user does not have access to the Repository where the Favorite is located. Therefore you cannot accidentally grant Repository permissions.
   - Verify that your Subscription contains only Favorites from Repositories that are available to the Role that is going to be using the Subscription.
   - Sometimes, if you are functioning in a Group Admin type Role or the System Admin Role, you have access to Repositories which another Role does not have access to.

     For example: Suppose you create a Subscription with a Favorite from Repository A and assign the Subscription to another Role, which only has access to Repository B and C. In this situation, the user would see the Subscription, but the Favorite would not be listed in the Reports tab because that user does not have access to it.

3. Assure Mainframe Security Access.

   - Verify that a particular user's mainframe credentials provide access to a CA View, CA Dispatch, or CA Bundl system and any particular data in one of those systems that is referenced in a favorite.
   - In the case of LDAP users, assure that their Profile has the correct security access in the mainframe repositories to access the data referenced by the Favorite.
   - In the case of LDAP Mainframe Hybrid Profile Object users, assure that their LDAP credentials are in sync with their mainframe credentials, and that their matching LDAP/mainframe credentials have the correct security access in the mainframe repositories to access the data referenced by the Favorite.

     Note: This access does not work with the built in LDAP mainframe hybrid profile object, because that profile forwards LDAP credentials to the mainframe. Therefor each LDAP user might be able to access different information, based on what their mainframe credentials have access to.

   Important! In no case does CA OM Web Viewer bypass mainframe repository level security.

4. Test the Role.

   Do one of the following:

   - Check the Role's Access using Mainframe Authentication

     - Assign yourself the Role in order to test it. (See User - Assigning Roles). This is a helpful practice, at least until you are more familiar with CA OM Web Viewer administration, and it is useful to check to be sure that your users do not run into problems.

       Note: Your site's security may restrict you from performing this test but you should still be able to perform the other steps in this procedure.

     - After assigning the Subscription to a Role, switch your current Role to the new Role in the After Login section of the Configuration tab to test how the user sees a subscription. (See Configuration – find exact section).

       This action lets you see if all the intended Favorites appear on the Reports page.

     Notes:

     Security for the CA View, CA Dispatch, or CA Bundl system still might block users from data you have access to. Be sure you only assign data to users that have access to the mainframe repository system.

     For example, in CA View, your mainframe credentials might have access to a Dist ID named ADMINST, but your users might not.

   - Check the Role's Access using LDAP Authentication.

     Logging into an LDAP authenticated Role might be difficult because you might not be able to validate your user account with the LDAP information that validates them.

     In this case, using the same Profile as that Role helps determine whether users of a Role will have access to the data you want them to be able to see and use.

     Assign the intended user’s Profile to a temporary Role, and assign yourself into that Role. Since the Profile you are using is now the same as the Profile their Role uses, your mainframe access should be the same as theirs.

     Also, your temporary Role needs access to the Repositories their Role has access to perform this test.

Connect a Subscription to a User Role

The reports listed on the reports page are based in part on the Subscriptions assigned to or owned by your Role. For Basic Users, all the reports they see are assigned to them in the form of Subscriptions.

Follow these steps:

1. From the Subscription Tab, click a Subscription.

   In the right pane, there are two lists, Available Subscriptions and Selected Subscriptions.

2. Select one of more Subscriptions in the Available Subscription list.

   Hold Ctrl or Shift while clicking to select more than one subscription

3. Do one of the following:

   - Click the single right arrow between the two lists to add the selected subscriptions
   - Click the double right arrow to add all the subscriptions to the Role.

4. Click Update at the top right of the pane.

   The Subscriptions are added to the Role.

Delete a Subscription from a Role

To remove a Subscription from a Role:

1. From the Administration tab, click the Role subtab
2. Click the Subscriptions subtab.

   There are two lists Available Subscriptions and Selected Subscriptions.

3. Select one of more subscriptions in the Selected Subscription list.

   Hold Ctrl or Shift while clicking to select more than one subscription.

4. Do one of the following:

   - Click the single left arrow between the two lists to remove one or more selected subscriptions.
   - (Optional) Click the double left arrow to remove all the subscriptions from the Role.

5. Click the Update button at the top right of the pane.

   The Subscription is removed.

How Subscriptions Are Displayed

Each Subscription a user has access to are displayed in the Reports tab.

The Subscriptions listed come from:

- Subscriptions you personally created
- Subscriptions assigned to your current Role

From the Reports tab, each Subscription is listed as a folder in left pane of the screen. You can expand the folder to see all the Favorites available from that Subscription.

The Subscription name listed in the Reports tab is the value entered in the Description field of the Subscription. For more information about setting the description see Create a Subscription Using Favorites.

Favorites in the Subscription may be listed differently, depending on the Favorite's type.

For example, certain Filter Favorites are actually displayed in a subfolder with a list of reports in that subfolder. For additional information, see How Favorites Are Displayed in Subscriptions.

Note: Some favorites from the Subscription may not be listed, if the user does not have access to the Repository the favorite refers to. It is an administration error to assign a favorite to a user that the user cannot access. For more information, see Assign a Subscription to a Role – Overview.

Report Actions from the Subscription List

You can complete several actions from the Action button in the Action column. The first steps are basically the same as editing the Favorite Properties. For more information about report actions, see Report Actions.

Additionally, you can browse the contents of a favorite by clicking its name in the Name column. For indexes, filters, and cross-report indexes, the format of data that appears in the subscription in the Reports tab is different than the data that are linked to it.

Note: Selecting a favorite for a report action can trigger a repository connection at runtime. If a repository connection fails because the user login credentials are invalid (for example, the password expires), CA OM Web Viewer prompts you for the new credentials to attempt another connection.

Managing Preferences

Use this section to set the following:

- General Preferences
- Display Preferences
- Output Default Preferences
- Auditing Preferences

Setting General Preferences

These general preferences apply to all CA OM Web Viewer users, including timeout (see page 81), maximum pages per search (see page 82), and the login and logout (see page 83) options. The settings in a user role or repository do not overwrite these settings.

Set the Timeout Settings

Use the Timeout section to specify user and remote connection timeouts.

User Timeout

If a user is idle for the number of minutes set, the session is automatically terminated.

Remote Connection Timeout

This is the connection timeout used when CA OM Web Viewer is communicating with the Mainframe repository systems through CA DRAS. This setting specifies how long CA OM Web Viewer should wait for a slow responding Mainframe or Repository or CA CCI connection before generating a timeout message.

Follow these steps to set timeout values:

1. From the Administration tab, click the Preferences subtab:
2. Click the General Preferences link.
3. In the Timeout section, set the options as follows:
   a. Locate the Logoff user after option and
   b. Enter the number of minutes that can lapse.

      The user is logged out of CA OM Web Viewer after this many minutes of idle time.
   c. Locate the Remote Connection timeout option.
   d. Enter the number of seconds that can lapse.

      CA OM Web Viewer-to-mainframe connection times out after this many seconds.
4. Click Update at the top right of the pane.

   The timeout values are updated.

Set the Maximum Pages Per Search Settings

The Maximum Pages Per Search affects the text search within reports.

When a user searches for a particular string of text in a report, the search normally continues until the end of the report if the search term is not found. However, in the case of extremely large reports, this can be time consuming and the user might not want to continue the search.

CA OM Web Viewer allows the user to break the search into segments. This setting controls the range of pages that can be searched at one time.

For example, if the limit is 10,000 pages, the first 10,000 pages are searched. The user is given the option to either continue or cancel the search.

Follow these steps to set the Maximum Pages Per Search:

1. From the Administration tab, click the Preferences subtab:
2. Click the General Preferences link and locate the Search section.
3. Enter the number of pages in the Maximum Pages per Search text box.

   The text search automatically breaks after this number of pages to see if the user wishes to continue.
4. Click Update at the top right of the pane.

   The Maximum Pages per Search value is updated.

Set the Login and Logout Settings

Use the Login/Logout section to specify password reset and confirmation dialog preferences.

Display Change Password

This setting determines whether you let Web Viewer users change their mainframe passwords through CA OM Web Viewer and when and if the change password display should be shown on the CA OM Web Viewer login screen.

Note: Users can only change their external security mainframe passwords. LDAP/EXIT password change is not supported.

There are three password change options:

Allowed

The users can change their mainframe password through the CA OM Web Viewer login page at anytime.

Note: LDAP users see the password change option, but are not able to use it. If you have both LDAP and Mainframe users, consider using the Only allowed after password is Expired option, which shows the password change dialog only after a user's external security expires.

With the Only Allowed after password expired option, LDAP/EXIT users never see the password change option, but Mainframe users see it when their password expires.

Not Allowed

The users are not allowed to change their mainframe passwords through CA OM Web Viewer.

Only Allowed After Password Is Expired

The users are allowed to change their mainframe passwords through CA OM Web Viewer, but only after their passwords have expired.

Note: LDAP users never see the password change panel. LDAP password change is not supported.

Confirm Logout

The Confirm Logout option is a general setting for all of Web Viewer that determines whether users have to confirm their logout. When the option is checked, the user is asked, "Are you sure you want to log off," after clicking the logout button. When the option is turned off, the user does not get a confirmation after clicking log out.

Follow these steps to set Login/Logout settings:

1. From the Administration Tab, click the Preferences subtab.
2. Click the General Preferences link and locate the Login/Logout section.
3. Locate the Login/Logout section.

4. Find the "Display change password" option.
5. Click one of the following radio buttons:
   - Allowed

     The User can change their mainframe password through CA OM Web Viewer.
   - Not Allowed,

     The User cannot change their mainframe password through CA OM Web Viewer.
   - Only Allowed after password is expired

     The User can only change their mainframe password through CA OM Web Viewer if it has expired.
6. Check or uncheck Confirm Logout.

   Specify whether your users are to receive a dialog asking whether they are sure they want to logout.
7. Click Update at the top right of the pane.

   Your Login/Logout preferences are updated.

Setting Display Preferences

Note: Display Preferences are also Performance Optimization Preferences.

All of these settings affect the amount of data presented to CA OM Web Viewer users. Although they are basically display settings, they can also be viewed as server tuning settings because they can affect the amount of bandwidth and memory each CA OM Web Viewer user can use. For more information, see the Best Practices Guide, Display Settings.

Reports per Report List Navigation

Controls the maximum number of reports listed on each report list and cross report report-section list.

A user performing a report search sees a maximum of this many reports. Similar to a "results per page" option, up to this many results can be shown on each page of a results list. The user can scroll to see the next group of reports.

For more information, see Report List, Cross Report List, and Cross Report Indexes.

Number of Pages per Request

The default number of pages of a report shown at one time.

For example, with a setting of 5, when a user is viewing a report, they see pages 1-5, providing there are five pages to display. Clicking Next displays the next five pages unless the end of the report is reached.

We recommend a default value of 5.

Notes:

- A lower number of pages per request reduces the impact on your network.
- Seeing a higher number of pages at once may increase usability if the user has to scroll through a large number of pages.

Maximum Number of Reports

The maximum number of reports that can be displayed on any single report list.

If a user searches for a very common report name, 100,000 reports might show up on the report list. This amount might be a waste of resources and is probably not very useful.

As a System Administrator, you can cap the maximum number of report results returned in a search. If the maximum results are capped at 2000, no matter how common the search term, only 2000 report names are returned.

We recommend setting a default value of 2000.

Notes:

- A lower maximum number of reports requested reduces the impact on system performance.

- If the user is trying to find a particular report, a narrower search criteria must be used.
- Avoid the misuse of resources by permitting large numbers of reports to be retrieved

For more information, see Best Practices – Display Settings.

Maximum number of value entries

The maximum number of index values that can be produced by a single search mask.

- Unlimited

  No limit on the number of index values entries that can be returned by a single search.

  Note:

  If a user searches a very common index such as SSN (social security number), several million index values could result. The user is not likely to need or use all those matches and time and system resources are wasted.

- Limited

  This places a cap on the number of index values that can be returned with a single search,

  With an upper limit of 200, only the first 200 matches are returned. If the user needs to find a result not listed in the first 200, the search criteria must be refined. For example, Ab* instead of A* or all phone numbers that are in a certain area code such as (987)* instead of all phone numbers.

We recommend Limited.

Follow these steps to change the Display Preferences settings:

1. From the Administration Tab, click the Preferences subtab:
2. Click the Display Preferences link.
3. Update the following text boxes.
   - Reports per report list navigation

     Enter the number of results you want to be listed per page.
   - Number of pages per request

     Enter the maximum number of report pages you want displayed at one time.
   - Maximum Number of Reports

     Enter the maximum number of reports to be listed in any single report list.
   - Maximum number of value entries

     Click Unlimited, or enter a value in Limited to set the maximum number of index value results returned.

4. Click Update at the top right of the pane.

   The Display Preferences are set.

Setting Output Defaults

To set output defaults, select Administration, Output Defaults.

These options set various defaults for printing (see page 88), emailing (see page 90), and file saving (see page 94). Many of these defaults can be overridden by the user, or Role based settings.

The user role controls whether a particular user can print, email or save, and sets limitations on those actions.

Printing Properties

CA OM Web Viewer supports these methods for printing reports:

- Print-friendly browser page
- Browser add-on

The print-friendly browser page offers near universal support. The browser add-on, which requires additional software installed on each end-user's computer, provides more capable printing, but may be blocked by browser or internet settings.

Method

Select the method for printing.

The print properties set here affect all users. Some of the settings can be overridden by the user at run time.

Printing Properties

Maximum Printed Columns (only for browser add-on)

When printing a report, you can limit the number of characters or columns a user can print on one line.

For example, if you set a limit at 120 columns or characters, any report the user printed would only print 120 characters on each line. Any remaining characters beyond the set limit would not get printed.

The values used for Landscape and Portrait printing do not have to be the same, and are set separately.

Fit to Page (only for browser add-on)

Specifies that the Fit to Page option is on by default

This option can temporarily be set on or off by the user at print time with the print dialog. However, the option always sets to this default when the user first logs into CA OM Web Viewer.

Default Point Size

Controls the default point size option on the print dialog

Point size controls the size of the font in the printed document. This option can temporarily be changed by the user at print time on the print dialog. However, this option always sets back to this default when the user logs in to Web Viewer.

Follow these steps to set or update printing properties:

1. From the Administration tab, click the Preferences Tab:
2. Click the Output Defaults link.
3. Select the print method. Choose Web Browser Printing to enable the print-friendly browser page.

4. Do one of the following tasks In Landscape, Don't Print After Column option to set or remove the column limit:
   - To set a limit
     a. Click the checkbox to enable the text box.
     b. Enter a value or use the up or down arrows to set the limit for the user's column print value.
   - To remove the limit, uncheck the checkbox.
5. Do one of the following tasks In Portrait, Don't Print After Column option to set or remove the column limit:
   - To set a limit
     a. Click the checkbox to enable the text box.
     b. Enter a value or use the up or down arrows to set the limit for the user's column print value.
   - To remove the limit, uncheck the checkbox.
6. Check or uncheck the Fit to Page option.

   Notes:

   - By default the print dialog shows Fit to page as checked if you check this checkbox.
   - If you uncheck this option, the print dialog shows the Fit to Page option as unchecked by default.
   - The user can change this option when they open the print dialog, but every time they log into CA OM Web Viewer, the option sets back to this default.
7. Set or adjust the Default Point Size.

   A user may have to log off and back onto the system before the new default becomes effective.
8. Click Update at the top right of the pane.

   The Printing Properties are updated.

Emailing File Options

The email properties set here affect all users, and all of these settings can be overridden by the user at run time.

Override considerations

- All of the options listed here are only defaults and can all be overridden at runtime by the user from the email dialog.
- Certain options can be overridden by Role settings:
  - If the user's Role is not allowed to email, the default options listed here do not affect that user. For more information, see Edit Role Properties - Report Actions
  - The default Text or PDF option can be overridden by options in a user's Role.

    If the user's Role is not allowed to email text reports as PDFs, a default file type of PDF is automatically overridden to be text. Alternately, if the user's Role is not allowed to email files as Text, the default Text to PDF option is PDF.
  - The options are the default options for email each time a user logs into CA OM Web Viewer.

    However, each time the user changes one of the options at the email dialog, that option remains changed for the rest of his session, unless he changes it again.

    The option resets to this default when the user logs out and logs back in.

Default File Type

When emailing a mainframe text report from CA OM Web Viewer, users can convert the mainframe text report to PDF or output the report as text.

Some users are allowed this option, based on the user's Role. However, if the user is allowed this option, this setting chooses the default option for them.

Those users who are allowed to change this option can change it from the default, but each time they log into CA OM Web Viewer the "Default File Type" setting sets back to this default.

PDF Options

The options selected on this panel are the default options used when any user opens the email document popup.

Note: This setting only affects users in Roles that permit them to convert text file to PDFs for an email. When a user who has PDF permissions is emailing a mainframe text document, the user can convert the document to PDF format, and is able to set several PDF options.

The PDF options include defaults for PDF font size, Page Orientation, and an option to use Green Bar background.

Follow these steps to set Emailing File Default Options

1. From the Administration Tab, click the Preferences subtab:
2. Click the Output Defaults link.
3. Find the Emailing File Options section.
4. Do the following In PDF options, according to your requirements.
   - Enter your Font size into the Font size points text box. Use the up and down arrows to scroll to your number.

     This size is the default PDF font size for emailing text reports.
   - In Page Orientation, click the Portrait or Landscape radio button.
   - Check or uncheck the Print Green Bar Background

     The alternating green and white bars in the background of a report may enhance readability.
5. Click Update at the top right of the pane.

   Your Email File Default Options are updated.

eMail Types

Web Viewer supports two methods for emailing reports:

- SMTP (web form)
- Browser add-on

The SMTP method offers universal support. The browser add-on, which requires additional software installed on each end-user's computer, provides more capable emailing by using the installed email client.

In order to enable the emailing of reports, select Client based MAPI and/or SMTP. If both email types are enabled, you can limit the email type based on the user role.

If a user's role allows both email options, the user chooses their email type from the configuration panel.

If you choose to enable SMTP email, the following settings are available. The information is supplied by your email system administrator.

SMTP Server

Specifies where the SMTP email server is hosted. Enter the name or IP address of the server.

Exchange Server

Check this box if you want CA OM Web Viewer to attempt to connect to your Microsoft Exchange Server so that your users can use the address book function on the SMTP email panel.

Note: The SMTP server that is listed is used for sending the emails. The Microsoft Exchange Server is only used for address book access.

With this option selected, CA OM Web Viewer automatically checks for your Microsoft Exchange Server in a number of locations.

Example:

SMTP Server: *yoursmtp.example.com*

Email: *employee@example.com*

If the CA OM Web Viewer server is connected to Active Directory with these settings, it will look at any service connection point (SCP) objects that the Microsoft Exchange Server published to Active Directory Domain Services.

The server will also look for Microsoft Exchange Server autodiscover servers in the following locations:

https://example.com/autodiscover/autodiscover + fileExtension

https://autodiscover.example.com/autodiscover/autodiscover + fileExtension

If no other results are produced, CA OM Web Viewer attempts to connect to the Exchange Server web services at:

https://yoursmtp.example.com/EWS/Exchange.asmx

Use Authentication

Specifies if the SMTP server requires user authentication. If selected, the end user is prompted for their email credentials.

Security Requires

If Use Authentication is selected, choose the security type: TLS or SSL.

port

If Use Authentication is selected, specify the port number.

File Saving

These settings are the default options for file saving. Normally, the user can overwrite these options when saving a file.

Override considerations

- All of the options listed here are only defaults and can all be overridden at run time by the user from the email dialog.
- Certain options can be overridden by Role settings:
  - If the user's Role is not allowed to save files, the default options listed here do not affect that user. For more information, see Edit Role Properties - Report Actions.
  - The default Text or PDF option can be overridden by options in a user's Role.

    If the user's Role is not allowed to save text reports as PDFs, a default file type of PDF is automatically overridden to be text. Alternately, if the user's Role is not allowed to save files as Text, the default Text to PDF option is PDF.
  - The options are the default options for file saving each time you log into CA OM Web Viewer.

    Optionally, the user can change options at the file save dialog and the options remain changed for the rest of his session, unless he changes the options again.

    The option resets to this default when the user logs out and logs back in.

Default File Type

When saving a mainframe text report from CA OM Web Viewer, users can convert the mainframe text report to PDF or output the report as text.

Some users are allowed this option based on the user's Role. However, if the user is allowed this option, this setting chooses the default option for them.

Those users who are allowed to change this option can change it from the default, but each time they log into CA Output Management Web Viewer the Default File Type setting sets back to this default.

PDF Options

The options selected on this panel are the default options when any user opens the save document popup.

Note: This setting only affects users who's Roles permit them to convert text file to PDFs during a save.

The File Save options include defaults for PDF font size, Page Orientation of PDF, and the option to have a Green Bar background in the PDF.

Follow these steps to set Save File Default Options

1. From the Administration Tab, click the Preferences subtab:

2. Click the Output Defaults link.
3. Find the File Saving File Options section.
4. Do the following In PDF options, according to your requirements and permissions.
   - Enter your Font size into the Font size points text box. Use the up and down arrows to scroll to your number.

     This size is the default PDF font size for saving text reports.
   - In Page Orientation, click the Portrait or Landscape radio button.
   - Check or uncheck the Print Green Bar Background

     The alternating green and white bars in the background of a report may enhance readability.
5. Click Update at the top right of the pane.

   Your File Saving options are updated.

Setting Auditing Preferences

Auditing provides a record of which users performed which action on the CA OM Web Viewer systems. This auditing lets the Systems Administrator control which actions are tracked in the Audit record.

For example, some sites might want to keep a record of when a user exported reports, and others might want to know when users logged in.

Considerations for setting Auditing User Actions:

- The System administrator would normally setup the auditing options before the users start to log into the system.
- Auditing of the targeted action for currently logged in users do not begin until the user logs out and then logs back into the system.
- All users newly logging on to the system have the action audited immediately.

Which User Actions to Audit

There are a number of different actions that can be audited. Each item represents an option or group of options for which auditing can be turned on or off.

The current actions in CA OM Web Viewer that are auditable are

- Annotation [for CA View only]

  This section includes:

  - Annotation - Add, change description, or delete
  - Note - Add, Change note access type (public/private), delete
  - Bookmark - Add or delete
- File Upload

  Uploading a file to the LPD server.
- Emailing of documents

  Attaching report data to an email
- Exporting of documents

  This section includes:

  - Exporting Data to a user's computer
  - Viewing report date from Export preview panel
  - Viewing report date based on report index/value combination from Export preview panel
- Printing of documents

  Sending reports to a user's printer
- Saving of documents

Saving reports to a user's computer.

- Viewing of documents

  This section includes:

  - Searching for search terms in Text Reports
  - Displaying report data from Text Reports
  - Displaying report data from other Non-text Report
- User logged in time

  This section includes:

  - User Logging in including Log in failure details
  - User Logging out
- Edit comments in report list [CA View only]

  Changing a report's comment attribute.

Audit Log File Options

Log File

The log file is a comma separated value file (CSV). This log file can be found in the "web" directory of your current CA OM Web Viewer deployment. The name of this file is in the following format:
auditRecord_MM_DD_YYYY.csv,

Where

MM is the month, DD is the day, and YYYY is the year that the report was created.

File Rolling

CA OM Web Viewer allows you to determine if you want a rolling log file. With the rolling log file option, you automatically get a new log file after the period of time specified. You can have a new audit log file daily, weekly, or monthly.

Without the audit log rolling all auditing information is put into one file.

Follow these steps to set auditing preferences:

1. From the Administration Tab, click the Preferences subtab.
2. Click Auditing Settings link.
3. Check or uncheck the following auditing preferences:
   - Annotation

     This choice is valid for CA View only.

     - Annotation

       This choice is valid for CA View only.

- File Upload
- Emailing of documents
- Exporting of documents
- Printing of documents
- Saving of documents
- Viewing of documents
- User logged in time
- Edit comments in report list
- This choice is valid for CA View only

4. Locate the Log File section.

   If you want to keep a rolling log

   a. Check the Yes button

   b. Select a rolling file increment for the log.

      If you select weekly, there is a new log file for each week.

5. Click Update at the top right of the pane.

   The Auditing Preferences are updated.

Viewing Auditing Preferences

When an action is audited, record of that action can viewed in two places:

- The Audit Log Panel
- A CSV in the web directory of your current Web Viewer deployment.

  For more information about viewing the audited information see the Audit Log in Web Statistics.

Statistics

The statics panel lists some basic statistics about this CA OM Web Viewer system.

Version

The current version of Web Viewer running

OM Webviewer Start Time

The last time the Web Viewer server was started

Logins Since Server Started

The number of logins since the server was started

Logins Since Product Installed

The number of logins since the product was installed

Total Number of User Accounts

The number of users defined in Web Viewer since the product was installed.

Number of Users Sessions Currently Online

The number of user that are currently logged on to Web Viewer

Exporting and Importing Admin Settings

CA OM Web Viewer lets you complete the following tasks:

- Import (see page 101) and export (see page 100) Repositories, Roles, Profiles, Users (see page 102), Directories, and Preferences.

  For example, you can export a Repository from one CA Output Management Web Viewer system as a backup, and then you import it into another system.
- Import many users into the system from an external formatted XML file.
- Upgrade (see page 102) the product from a previous release.

Important! Do *not* use this export feature in place of regular backups of your CA Output Management Web Viewer database. This feature does not export system preferences, favorites, and other runtime objects that the CA Output Management Web Viewer database stores. For more information about how to back up your CA Output Management Web Viewer database, see your database product documentation.

More information:

Import Users (see page 102)
Import CA Output Management r11.5 Update (see page 102)

Export Admin Objects

You can export administration objects for use in other CA Output Management Web Viewer systems.

Follow these steps:

1. On the Administration tab, click the Repository subtab, if necessary.

   Note: The same export dialog is displayed from the Repository, Role, Profile, Directory, and User tabs. You can open the dialog from any of these subtabs.

2. Click Export, select one or more of the following optional objects that you want to display, and click Next.

   - Repository
   - Role
   - Profile
   - User
   - Directory
   - Preferences

   A prompt to download an XML file for the first selected object type appears.

3. Click Save and specify a save location.

   The file contains an XML representation of the objects of the selected type in your database.

   If multiple objects were selected in step 2, a prompt to download an XML file for the next selected object type appears.

4. Repeat step 3 for each selected object type.

5. (Optional) Click Retry to restart the download from the previous pane.

6. Click Finish.

Import Admin Objects

You can import admin objects from CA Output Management Web Viewer.

Follow these steps:

1. On the Administration tab, click the Repository subtab, if necessary.

   Note: The same import dialog is displayed from the Repository, Role, Profile, Directory, and User tabs. You can open the dialog from any of these subtabs.

2. Click Import and select one or more types of objects for import.
3. Click Browse and locate the XML file for each type of admin object that you want to import.
4. Select one of the following Conflict options for each import file:

   Override

   Overrides the attributes in any existing object. For example, you import any object with the same name and type as an object already in the database.

   Important! This option does not overwrite an object completely. If the object that you import does not contain certain attributes, the attributes are taken from the overridden object.

   If the attribute is a list style, such as a list of Roles to which a user has access, the lists in the overridden object and the overriding object are combined. The Roles a user is given access to from the imported user object combine with the Roles the user already has access to in CA OM Web Viewer.

   Skip

   If the object exists with the same name and type as the object being imported, the object is not imported.

   Duplicate

   (Allowed only for Role and Repository type objects)

   If the object exists with the same name and type as the object being imported, the tool modifies the object name and adds it to the database.

5. Complete steps 3 and 4 for each object that was selected in step 2.
6. Click Import.

   A confirmation or error message displays.

7. Continue importing more objects or click close to close the dialog.

Import Users

The user import follows the same procedure as importing any admin import.

Note: We recommend that you export a single user object to see the user object format. Then, use that format to build your list of users.

Follow these steps:

1. Export Single User.
2. Open the User Export File with a text or xml editor.
3. Duplicate the user entry for each user you want to import to the system.
4. Change the user personal information, which you want to be unique to the user.
5. Change the user role assignments, if you want to add the user as a member of one or more specific roles.

   Note: You would normally use an automated process for producing this XML file. Contact CA Technologies Services, if you want to have CA Technologies produce an XML file containing your user list.
6. Import the file.

More information:

Export Admin Objects (see page 100)
Import Admin Objects (see page 101)

Import CA Output Management r11.5 Update

The CA OM Web Viewer r11.5 Database Export tool exports your settings from the CA OM Web Viewer r11.5 application. The XML files that are generated by the CA OM Web Viewer r11.5 Database Export tool are then imported into the current CA OM Web Viewer using the import feature.

Note: For more information about upgrades, see the *Installation Guide*.

More information:

Import Users (see page 102)

Chapter 3: Viewing Web Statistics

The Web Statics tab provides the following:

- Admin Info (see page 104)

  Provides basic statistics about this CA OM Web Viewer system since the installation.

- Repository Status (see page 105)

  Provides a list of the repositories and status information.

- User Status (see page 107)

  Provides information about the currently logged on CA OM Web Viewer users.

- Audit Log (see page 107)

  Provides a listing of each audited user action.

This section contains the following topics:

Viewing Admin Info (see page 104)
Viewing the Repository Status (see page 105)
Viewing the User Status (see page 107)
Viewing the Audit Log (see page 107)

Viewing Admin Info

View Admin Info and review basic statistics about this product installation.

Follow these steps:

1. From the Web Statistics tab, click Admin Info.
2. Review the following information:

   Version

   Specifies the current version of CA OM Web Viewer.

   OM WebViewer Start Time

   Specifies the last time that you started CA OM Web Viewer.

   Logins Since Server Started

   Specifies the number of logins since you restarted the server.

   Logins Since Product Installed

   Specifies the number of logins since you installed the product.

   Total Number of Users Since Product Installed

   Specifies the number of defined users in CA OM Web Viewer since you installed the product.

   Number of Users Sessions Currently Online

   Specifies the number of users that are currently logged on to the server.

Viewing the Repository Status

The Repository Status panel provides a Systems Administrator with a list of all the repositories, and whether they work correctly. If the product suspects a system problem, you can check the status icon. The icon tells you about the availability of the CCI server, the DRAS server, and the repository instantly.

Note: The Repository status check occurs in real time. If you defined many repositories, this panel can take longer to display. If a CCI or DRAS failure blocks several systems, the status checks can take longer, but can also timeout each repository.

 (Normal)

Shows that the CCI server, DRAS server, or repository is up and working correctly.

 (Problem)

Shows that the CCI server, DRAS server, or repository is either not available or reachable.

Repository Name

Lists the names of the repository objects that are defined on the system.

These repository names match the repository object names defined when an administrator creates a repository object at the Create Repository Panel.

Domain Connection

The primary location of the repository objects.

Displays information about whether each part of the connect path (CCI server, DRAS server, and repository) to that repository object is reachable and up. Each object must point to at least one repository location--the primary location that is defined in the Repository panel.

Note: A *repository location* consists of one mainframe system ENF id, one DRAS system, and one View, Dispatch, or Bundl system. Only the primary location of the repository is listed in this section, although the repository can also have alternate locations.

The Domain Connection has columns for the CCI Server, the DRAS Server, and Repository:

CCI Server

Lists the Event Notification Facility (ENF) ID. The CCI server that you use to try to connect to a repository also uses this ID.

When the Mainframe, ENF, or CCI server is down, the problem icon displays in this column. The following columns also show a problem symbol because the DRAS server and the repository are unreachable through this CCI server.

Note: If the CCI server is down and you are unable to connect to a certain repository, even though the repository object is unreachable, it may actually be up and working correctly. The CCI server can make the repository appear to be down.

DRAS Server

The CA Distributed Repository Access System (CA DRAS) for each repository.

When a DRAS server is down or unreachable, the problem icon displays in this column. The Repository column that follows also shows a problem symbol, because it cannot be reached through that DRAS server.

Note: A repository following a DRAS server that appears down can actually be running correctly, but cannot be reached because the connection is down.

Repository Name

Represents a CA View, CA Dispatch, or CA Bundl repository. The ACCESS REPOSITORY statement defines the name in the DRAS configuration of the DRAS being used to connect to this repository.

For more information on any of the connection parts see Creating a new Repository Object, the Location Address Explanation section.

Follow these steps:

1. From the Web Statistics tab, click the Repository status subtab and view information about the repositories and connections.
2. (Optional) If the server or repository does not display, perform one of the following steps:
   - To view more pages, use the navigation arrows at the top left corner of the pane, and scroll the page from left and right.

     To the left of the navigation arrows is a numerical display showing the total number of pages of repositories. If there are less than 20 repository objects, these arrows do *not* appear.
   - Use the Find command in your browser.

Viewing the User Status

The User Status panel shows information about the currently logged on CA OM Web Viewer users.

Note: If you are running several CA OM Web Viewer servers in a server balancing setup, you only see information about users on this particular server. You do not see users from all the servers in a server farm.

You can instantly see the users who are currently online on this server instance (user sessions are tiered at the web server level), and some basic information about their current access. Listed data includes IP addresses, the repositories they are accessing, when the last Repository access was granted, and the role that was being used.

Follow these steps:

1. From the Web Statistics tab, click the User Status subtab.
2. Review the attributes that display for the currently logged on users:

   User ID

   Specifies the product ID for that user

   Last Access Time

   Specifies the last time that the user accessed the repository data.

   Last Repository Access

   Specifies the last repository that the user accessed.

   IP Address

   Specifies the IP address, and host name (if available) of the end-user computer.

   User Role

   Specifies the role of the user.

Viewing the Audit Log

The Audit log can be a valuable debugging tool. Each successful user action that is audited is shown in this panel. The choice of actions to be audited is controlled from the Auditing Settings panel. Each user action is one row in the table and each column is an attribute that can be used to get information about the audited action. Some columns may not contain any information.

For more information, see Setting Auditing Preferences.

Follow these steps:

1. From the Web Statistics tab, click the Audit Log subtab.
2. Review the following attributes that describe action instances.

This log displays all the Audit Attributes of the Repositories and connections that CA OM Web Viewer uses.

The panel lists each attribute for every audit action, but some audit actions may not fill all the attribute columns. For example, a login event is not associated with any particular Report ID. Therefore, the audit item of a login does not list a value for the Report ID field.

Date & Time

Specifies the date and time of the action.

User ID

Specifies the user ID who performed the action.

Remote ID

Specifies the mainframe ID or profile ID used for this user when the user connected to a repository.

IP Address

Specifies the IP address, and host name (if available) of the end-user computer.

User Role

Specifies the role of the user who performed the action.

Repository Name

Specifies the name of the repository object where the action was performed.

Repository Location

Specifies the location string for the repository object that was acted upon.

For more information, see Creating a New Repository Object, the Location Address Explanation.

Report ID

Specifies the report ID that was acted upon.

Action

Specifies the action that the user performed.

For more information, see Setting Auditing Preferences.

Starting Page

Certain operations, such as viewing data, include the page number of the first page viewed. For example, if you viewed 6-10 of reports, the start page would be 6, and the total pages viewed would be 5.

Total Page(s)

Certain operations, such a viewing data, include total number of pages include in this action. For example, if you viewed 6-10 of reports, the start page would be 6, and the total pages viewed would be 5.

Details Connection Duration

Displays details about an action performed. For example, when viewing an indexed section of a report, this column lists the type of report along with the index name and selection.

Connection Duration

Specifies the amount of time CA OM Web Viewer spent to complete the task. Time does not include data transfer time between the end-user computer and CA OM Web Viewer.

Chapter 4: Configuring

The configuration settings are user settings, similar to options or preferences. Configuration settings only apply to you as a user and can be customized according to your personal preferences.

Typically, these settings do not have to be changed, but customizing them according to your environment can save time and enhance efficiency.

This section contains the following topics:

Managing the Default Repository Filter Settings (see page 111)
Managing the Report List Display Settings (see page 117)
Managing the Favorites List Display Settings (see page 120)
Managing the Report Level Actions Settings (see page 123)
Managing the After Login Settings (see page 127)
Managing Your Credentials (see page 130)

Managing the Default Repository Filter Settings

These topics include procedures for modifying default filter settings.

Note: These settings are only available to System and Group Administrators and Advanced Users.

All of these settings affect the advanced search defaults and behavior. The default filter settings let you set the defaults for finding reports and cross-report indexes.

Important: If enabled, the default settings set here override the default filter settings for every Repository.

Update Date and Version Criteria

In CA OM Web Viewer, you can search for reports based on either creation date or version. This section explains how to set or modify the defaults for Date and Version Criteria.

Note: For these defaults to override Repository level settings, select Restore Filter Settings with these user settings after login.

Follow these steps:

1. From the Configuration Tab, click the Repository Filter link in the left pane.

   The Repository Filter pane appears.

2. Click the Repository Filter link in the menu on the left side.
3. Click the Date & Version Criteria Tab.
4. (Optional) Select Creation Date to set the default search range for reports by the reports' archive dates.

   Do one of the following to specify search criteria:

   - Select the Creation Date and specify a value for the Days Ago default search criteria.

     Enter a number of days you want to include. For example, 50 days would show the last 50 calendar days worth of reports.

     Note: These reports do not include reports archived in the current day if the report was archived in a time zone that time stamped the report's date of the archive of the report a day forward from your current date.

   - Select Between and do the following:

     a. Set the Start Date in the first text box:

        Click the calendar button and select a date from the calendar pop-up or enter a start date in the first text box.

     b. Set the End Date in the second text box.

        Click the calendar button and select a date from the calendar pop-up or enter a start date in the second text box.

5. (Optional) You can search for various versions of a report.

   Select one of the following options to set defaults for Versions :

   - All

     All versions of a report are shown but might not include offline-reports.

   - Latest

     Enter a number of versions to display.

This option controls the number of versions of the report that are displayed by default. For example, if you select five, the most current five versions of the report are displayed. If you have less than five versions, all versions are displayed.

- Range From

  All versions in this range are displayed, by default.

  - Enter a number for the first version of the report to be displayed.
  - Enter a number for the last version of the report to be displayed.

6. (Optional) Update your filter preferences according to your requirements.

   There are several generic filter settings that affect all the defaults described on this pane. These options apply to both Report Searches and Cross-Report Index searches.

   - Select Show Filter Settings

     Controls whether you want your current search criteria to be displayed on the Report Search and Cross-Report Index Search panes.

     If left clear, the Automatically Apply Filter settings is automatically selected.

     With Show Filter Settings left clear, the result is that all searches use your default settings from this pane, and you are not given the option to change filter criteria from the search pane--the search options are not even shown.

   - Select the Automatically Apply Filter Settings

     Specifies that the search is automatically run when you go the search pane.

     If you don't automatically run the search, the search criteria must be shown at the search pane. (See Previous Step)

     If left clear, the Show Filter Setting and Restore Filter settings with these user settings options are automatically selected.

   - Restore Filter Settings with these User Settings

     Determines whether the settings on this pane are to override the Repository settings.

     If selected, these settings are used; if left clear, the default Repository settings are displayed as the search criteria.

7. Click Update in the upper right corner of the pane.

   The Date and Version default criteria are updated.

Update Report Criteria

Use this pane to set the defaults for Report Criteria.

Note: For these defaults to override the Repository level settings, select the Restore Filter Settings with these user settings after login option.

Follow these steps:

1. From the Configuration Tab, click the Repository Filter link in the left pane.

   The Repository Filter pane appears.

2. Click the Report Criteria subtab.

   Set or update the following optional values:

   Report ID

   Enter a default Report ID name, or a search string with wildcards to display multiple reports.

   Mode [CA View only]

   Limit the reports to only those reports that are viewable from a specific CA View mode.

   Dist ID [CA View only]

   Limit your reports to only those reports that are viewable from a specific CA View Distribution ID

   Mail Code [CA Bundl only]

   Limit your reports to only reports viewable from a specific CA Bundl Mail Code.

   Recipient [CA Dispatch only]

   Limit your reports to only reports viewable from a specific CA Dispatch Recipient.

   On-line reports only

   Select On-line Reports Only. If left clear, off line reports are also included in your report searches.

3. (Optional) Update your filter preferences according to your requirements.

   There are several generic filter settings that affect all the defaults described on this pane. These options apply to both Report Searches and Cross-Report Index searches.

   - Select Show Filter Settings

     Controls whether you want your current search criteria to be displayed at the Report Search and Cross-Report Index Search panes

     If left clear, the Automatically Apply Filter settings is automatically selected.

     With show filter settings left clear, the result is that all searches use your default settings from this pane, and you are not given the option to change filter criteria from the search pane--the search options are not even shown.

   - Select Automatically Apply Filter Settings

     Specifies that the search is automatically run when you go the search pane. If you don't automatically run the search, the search criteria must be shown at the search pane. (See Previous Step)

     If left clear, the Show Filter Setting and Restore Filter settings with these user settings options are automatically selected.

   - Select Restore Filter settings with these user settings

     Determines whether the settings on this pane are to override the Repository settings.

     If selected, these settings are used; if left clear, the default Repository settings are used.

4. Click Update in the upper right corner of the pane.

   Your report criteria default filter settings are updated.

Update Index Criteria

Use this pane to set the defaults for Index Criteria. These settings affect your Cross-Report Index searches.

Note: For these defaults to override the Repository level settings, select the Restore Filter Settings with these user settings after login option.

Follow these steps:

1. From the Configuration tab, click Repository Filter in the left pane.

   The Default Filter Settings pane is displayed.

2. Click the Index Criteria subtab.

   The Index Criteria pane is displayed.

3. (Optional) Set or update the following values:
   - Set the case of the text. Do one of the following:
     - Select As Uppercase – Treat whatever text is added to the index name and index value text boxes as uppercase. The text you enter is converted to uppercase.
     - Select As Typed – Treat whatever text is added to the index name and index value text boxes as the original case.

       The text you enter is not converted to uppercase.
4. Enter values for your Indexes in Names and Values.

   This index or index combination is your default index search.
5. (Optional) Update your filter preferences according to your requirements.

   There are several generic filter settings that affect all the defaults described on this pane. These options apply to both Report Searches and Cross-Report Index searches.
   - Select Show Filter Settings

     Controls whether you want your current search criteria to be displayed at the Report Search and Cross-Report Index Search panes.

     If left clear, the Automatically Apply Filter settings is automatically selected.

     The result is that all searches use your settings from this pane, and you are not given the option to change settings from the search pane--the search options are not even shown.
   - Select Automatically Apply Filter Settings

     Specifies that the search is automatically run when you go the search pane.

     If you don't automatically run the search, the search criteria must be shown at the search pane. (See Previous Step)

     If left clear, the Show Filter Setting and Restore Filter settings with These User Settings options are automatically selected.
   - Restore Filter Settings with these user settings

     Determines whether the settings on this pane are to override the Repository settings.

     If selected, these settings are used; if left clear, the default Repository settings are used.
6. Click Update in the upper right corner of the pane.

   The Date and Version default criteria are updated.

Managing the Report List Display Settings

Note: This function is only available to Advanced User, Group Administrator, or System Administrator roles.

The list layouts section controls the default layout in the advanced search reports list and in the report list generated by the cross-report indexes. The layout options include the ability to do the following:

- Define which attribute columns you see
- Set the display order of the columns
- Specify the column to sort by

Considerations:

- If you do not select the Override the Report List Layout Set by Administrator option, none of these settings apply.
- If you have unusual usage or need extra features, select the Override the Report List Layout Set by Administrator option so that these options override the defaults.

  The column settings listed in the Report List Layout are used to override the Repository defaults set by the administrator.

Note: Both the Advanced Search Report List and the Cross-Report Index Report List must have at least one column included. Beyond that, you can select or not select any of the attributes columns listed in the Available Report Columns list.

Update the Report List Layout

You can update the layout of the Report List. The three procedures described in this section explain how to:

- Set the default selected report columns for the default repot list column
- Change the display order of the attribute columns.
- Set the default sort column and default sort order.

Note:

- Changing these settings affects both the Report List in Advanced Search, and the Cross-Report Indexes list.
- These settings do not override the report list layout set by the administrator, unless you select Override the Report List Layout Set by Administrator option.

How to set the selected report columns for the default report list

Follow these steps:

1. From the Configuration Tab, click the Report List link in the left pane.

   The Report List Layout pane appears.

2. Select one of more attribute column names in the Available Report Columns.

   (Optional) Hold Ctrl or Shift while clicking to select more than one attribute column name.

3. Do one of the following:

   - Click the single right arrow between the two lists to add the selected attribute columns.
   - Click the double right arrow to add all the attribute columns.

4. Click Update in the upper right corner of the pane.

   The column list is updated.

Note: The attribute columns listed in the Selected Report Columns are the default columns listed in a user's Advanced Search Report List and also the Cross-Report List.

How to set the order of the attribute columns

Follow these steps:

1. From the Configuration Tab, click the Report List link in the left pane.

   The Report List Layout pane appears.

2. Find the Report List Layout section, then Selected Report Columns list.
3. Click on a column and use the up and down arrows to position the selected column in the display.
4. Click Update in the upper right corner of the pane.

   The display order is updated.

How to set the sort order

Follow these steps:

1. From the Configuration Tab, click the Report List link in the left pane.

   The Report List Layout pane appears.

2. Select an attribute column name from the Sort Report List By drop-down list.
3. Select Ascending or Descending sort order
4. Click Update in the upper right corner of the pane.

   The sort order is updated.

Show Advanced Options

Use this option to control whether the Advanced Options menu is displayed in the Cross-Report List and Advance Search Report List.

The advanced options drop-down list is displayed as a column labeled Action that has an Action button for each report. From this Action button drop-down list you can select various advance options to perform on a report, such as show report information, update report comment, browse in new window, print, email, save, export, and index selection on AFP reports.

Note: Unlike many of the settings on this section, this setting does not have a repository level default.

Follow these steps:

1. From the Configuration Tab, click the Report List link in the left pane.

   The Report List Layout pane appears.

2. Find the section below the Report List Layout section
3. Select or clear the Show Advanced Options drop-down option.

   Note: Unlike many of the settings in this section, this setting does not have a repository level default. The option you select is your personal option.

4. Click Update at the top right corner of the pane.

   The options are updated.

Override Report List Layout Settings

Use this setting to control the override of the report list layout.

The Override the Report List Layout Set by Administrator option controls whether the layout settings from this pane override the Repository defaults.

Follow these steps:

1. From the Configuration Tab, click the Report List link in the left pane.

   The Report List Layout pane appears.

2. Find the section below the Report List Layout section.
3. Select or clear the Override the Report List Layout set by Administrator option.

   If selected, the defaults settings in the Report List Layout are used. If left clear, the default layouts for each Repository, which are set by the Administrator, are used.

   Note: You must have at least one of the Available Report attribute columns in the Selected Report Columns pane.

4. Click Update at the top right of the pane.

   The override setting is updated.

Managing the Favorites List Display Settings

Note: This setting is only available to an Advanced User, Group Administrator, or System Administrator.

Use the list layouts section to control the default layout in the advanced search favorites list and on the Subscription Creation pane. In this section you can:

- Define which attribute columns you see
- Set the display order of the columns
- Specify the column to sort by

The column settings in the Favorite List Layouts are used to override the Repository defaults set by the Administrator. If you have unusual usage, or need extra features, you may choose to override these settings. Select the Override the Report List Layout set by Administrator option for these settings to take effect..

Both the Subscription creation Favorites List and Advanced Search Favorites List must have at least one column included. Beyond that you can select or not select any of the attributes columns listed in the Available Favorite Columns list.

Update the Favorite List Layout

You can modify the default settings for favorites. The three procedures described in this section show you how to:

- Set the Available Favorite Columns for the default Favorite List
- Change the display order of the attribute columns:
- Set the sort column and the sort order

Note:

- Changing these settings affects both the Subscription Creation List and the Advanced Search Favorite List.
- These settings do not override the favorite list layout set by the administrator, unless you select the Override the Report List Layout Set by Administrator option.

How to set Available Favorite Columns for the default Favorite List Layout

Follow these steps:

1. From the Configuration Tab, click the Favorite List link in the left pane.

   The Favorite List Layout pane appears.

2. Select one of more attribute column names in the Available Favorite Columns.

   (Optional) Hold Ctrl or Shift while clicking to select more than one attribute column name.

3. Do one of the following:

   - Click the single right arrow between the two lists to add the selected attribute columns.
   - Click the double right arrow to add all the attribute columns.

   Note:

   - The attribute columns listed in the Selected Favorite Columns are the default columns listed in your Subscriptions page and Favorites page.
   - You must have at least one of the optional attribute columns in the Selected Report Columns pane.

4. Click Update in the upper right corner of the pane.

   The column list is updated.

How to set the order of the attribute columns

Follow these steps:

1. From the Configuration Tab, click the Favorite List link in the left pane.

   The Favorite List Layout pane appears.

2. Find the Favorite List Layout section, the Selected Favorite Columns list.
3. Click on a column and use the up and down arrows to position the selected column in the display.
4. Click Update in the upper right corner of the pane.

   The display order is updated.

How to set the sort order

Follow these steps:

1. From the Configuration Tab, click the Favorite List link in the left pane.

   The Favorite List Layout pane appears.
2. Select an attribute column name from the Sort Favorite List By drop-down list.
3. Select Ascending or Descending sort order
4. Click Update in the upper right corner of the pane.

   The sort order is updated.

Show Advanced Option for Favorites

Use this option to show or hide the advanced options in the Favorites List.

This option controls whether the Advanced Options menu is displayed in the Subscription Creation Favorite List and Advance Search Favorite List.

On those lists, the Advanced Options drop-down list appears as a column labeled Action that has an Action button for each report. From this Action drop-down list, you can select various advance options to perform on a report including:

- Favorite Properties, View Report Information
- Browse, Browse in New Window
- Remove Favorite
- Print, Email, Save, and Export

Important! This setting does not have a repository level default, and therefore is not overwriting a repository default. It does however apply to all repositories.

Follow these steps:

1. From the Configuration Tab, click the Favorites List link in the left pane.

   The Favorite List Layout pane appears.
2. Find the section below the Favorites List Layout section.
3. Select or clear the Show Advanced Options in the favorites option.
4. Click Update at the top right corner of the pane.

   The options are updated.

Override Favorite List Layout Settings

Use this option to set the Override the Favorite List Layout set by Administrator option. This option determines whether the layout settings from this pane override the Repository defaults.

Follow these steps:

1. From the Configuration Tab, click the Favorites List link in the left pane.

   The Favorite List Layout pane appears.

2. Find the section below the Favorite List Layout section
3. Select or clear the Override the Favorite List Layout set by Administrator option.

   If selected, the defaults settings in the Favorite List Layout are used. If left clear, the default layouts for each Repository, which are set by the administrator, are used.

   Note: You must have at least one of the Available Favorites attribute columns in the Selected Favorite Columns.

4. Click Update at the top right corner of the pane.

   The override setting is updated.

Managing the Report Level Actions Settings

This section includes:

- Report Browsing Settings
  - Text Size
  - AFP Conversion Options
- SMTP Email Options

  Note: You cannot see the SMTP options if your administrator did not enable SMTP email.

Configure Report Browsing

Use this pane to update your report level actions for report browsing and transformation.

Note: In past versions of CA OM Web Viewer, users had to choose the option to convert AFP to PDF at browse time. This setting replaces the task of having to make a choice at each browse. However, if you want to change your choice, you have to reconfigure this setting.

You can do the following:

- Set text size
- Specify if an AFP report is to be transformed to PDF or kept as AFP.

  CA OM Web Viewer can automatically transform AFP reports into PDF files if your administrator allows this option.

Follow these steps:

1. From the Configuration Tab, click Report Action link in the left pane.

   The Report Level Action pane is displayed.

2. Find the Text Size option, click the Text Size drop-down list, and select a size.

   This Text Size option controls the font size on all the report browsing pages you have available to you in your current role.

3. Find the Transform AFP Report.

   Note: The administration options set for your current repository override these options. These options are only used for repositories where the administrator allowed the User Choice (AFP or PDF).

   For more information, see the Administration tab, Repository object, Set Automatic Transformation of AFP Report to PDF section.

4. Do one of the following:

   - Click Keep as AFP

     When allowed, keep AFP report in AFP format.

   - Click Convert to PDF

     When allowed, transform the AFP files to PDF files automatically.

5. Click Update at the top right of the pane.

   The Report Level Actions are updated.

eMail Type

If your administrator has allowed both SMTP email and browser add-on, you can choose to use either the browser add-on or SMTP (web form) to perform the action. If the administrator has not allowed both types of email, this section is not displayed.

The browser add-on, which uses your installed email client, is the default method. However, the browser add-on may not be available due to your browser or internet settings. In that case, you can use SMTP.

SMTP Email Account

If your administrator has selected SMTP email, you can set up your default SMTP information so that you do not have to enter it into the email dialog each time you want to email a file.

If your administrator setup CA OM Web Viewer to use the Microsoft Exchange Server address book, you are required to enter your SMTP information in order to access the address book.

Note: If your administrator did not select CA OM Web Viewer SMTP Email, this section is not displayed.

The following SMTP settings are available. The information is supplied by your system administrator.

Credentials

You have two options, using your CA OM Web Viewer login credentials or entering a username and password.

Note: Depending on how your administrator setup CA OM Web Viewer SMTP Email and whether the Microsoft Exchange Server address book is used, you may not be required to fill in this data. If it is not required, the credentials section is not displayed.

Domain

If you are using your CA OM Web Viewer login credentials, you can optionally append a domain name to the end of your username. For example, a username of UserID and a domain of example.com would be used to produce the email server username of UserID@example.com.

Username

The username for your account on the outgoing email server.

Password

Your email account password.

Email Address

The Email Address is the return address for your outgoing mails, usually your work email. This is the address your recipient will reply to.

If you are attempting to use the Microsoft Exchange Server address book, you have to enter an email address that is listed in the address book.

Note: Regardless of the address you define here, the email can be audit logged as coming from your account on CA OM Web Viewer.

Follow these steps:

1. Find the SMTP Email Account section.
2. Enter your credentials information.
3. Enter your email address.

Managing the After Login Settings

The After Login settings determine some basic defaults for access in CA OM Web Viewer including:

- The Role you are using
- The Repository you access by default
- Whether you want to show the Repository list

Change User Roles

The user Role is an important concept in CA OM Web Viewer and using different roles gives you varied abilities, permissions, and functions.

- Your current Role affects which Repositories and Reports you have access to in CA OM Web Viewer.
- Your Role can also affect the actions you are permitted to perform in CA OM Web Viewer such as printing, emailing, and so on.

The role you are currently using is listed at the top left side of the main CA OM Web Viewer pane to the right of your user ID.

For example, "Logged in as: jdoe @ Bank Teller Lvl III," means the user "jdoe" is logged in and the user's current Role is Bank Teller Lvl III.

You can select and change your current role based at any time, if you are assigned more than one Role.

Follow these steps:

1. From the Configuration Tab, click the After Login option in the left pane.
2. Find the User role drop-down list. Your current role is displayed in the text box.
3. Select the Role you want to use.

   All the Roles assigned to you are listed in this drop-down list. If you want to be added to another Role contact your System Administrator or Group Administrator.

   Note: Changing your current Role can reset your default Repository selection, if the Role you choose does not have access to the Repository you selected as your default.
4. Click Update at the top right corner of the pane.

   In some cases you can get logged out of CA OM Web Viewer and you have to log back in.

   This can happen when two of your Roles are authenticated by two different authentication methods.

More information:

Choose a Repository (see page 128)

Choose a Repository

Note: This setting is only available to an Advanced User, Group Administrator, or System Administrator.

This setting lets you define a default Repository. This is the Repository that is selected automatically when you go to the Advanced Search tab for the first time. If you frequently use a specific Repository, this might be an efficient setting because the Repository selection step is automatically completed.

Note: You can still access other Repositories by clicking on their respective links in the Repository list in the Advanced Search tab.

Repository selection works this way:

- The default Repository automatic selection occurs only the first time you go to the Advanced Search pane after log in.
- After you select another Repository at the Advanced Search tab that Repository remains selected until another Repository is selected or you log out.
- The next time you log into CA OM Web Viewer, the default selection is again selected when you go the Advanced Search pane.

Follow these steps:

1. From the Configuration Tab, click the After Login Link in the left pane.
2. Find the Repository drop-down list. The current default Repository is displayed
3. Select a default Repository from the Repository drop-down list. Only repositories available to your current Role are listed in the drop-down list.

   Note: This setting can be reset by selecting a Role that does not have access to this Repository. When you click Update, the Role and Repository are reset.
4. Click Update at the top right corner of the pane.

   The value for Default Access Repository is updated.

More information:

Change User Roles (see page 127)

Show Repository List

Use this option to control whether the Repository list is shown or hidden by default on the Advanced Search pane.

Note: Regardless of this setting, you can hide or show the Repository list from the Advanced Search pane.

Use this option in these situations:

- If you only have one Repository available to you or rarely change Repositories

  It may be helpful to hide the Repository list to gain more screen space. You can expand the Repository list from the Advanced Search pane, if you need to change your Repository.

- With a Default Repository selection

  If you use this option, you do not have to expand the Repository list to choose a Repository each time you log in.

- With the Automatically Apply Filter Settings option from Repository Filter settings

  You can have a Report list generated for your chosen Repository.

Follow these steps:

1. From the Configuration Tab, click the After Login Link in the left pane.
2. Select the Show Repository List option.

   The default is set for the Report List.
3. Click Update at the top right corner of the pane.

   The option is updated.

Managing Your Credentials

Use the Credentials pane to control your mainframe credentials. You can use your CA OM Web Viewer login credentials for all repositories, or you can use individual credentials for each repository you have access to in CA OM Web Viewer.

Typically, with external security enabled, all your accessible repositories use the same user id and password. However, for certain system setups, your administrator can assign repositories with internal security that requires a different set of credentials. In this case, your system administrator can help you with the required credentials for each system.

Notes:

- This function is available only for the Advanced User, Group Administrator, or System Administrator roles.
- This function is not available for the Exit-Authenticated users with External Security EXIT authentication.
- By default, CA OM Web Viewer uses your CA OM Web Viewer login credentials as your credentials to all repositories. To access reports or repositories, mainframe credentials are required. If the credentials become invalid at runtime, CA OM Web Viewer prompts you for new credentials to attempt another connection.

  For mainframe security reasons, your account can be suspended after a specified number of unsuccessful connection attempts with invalid credentials. The number is specified by your security administrator.

Set the Default and Individual Credentials for Repositories

To set your login credentials, use the Credentials pain. Credentials let you access each repository that you want to view.

Follow these steps:

1. From the Configuration Tab, click Credentials in the left pane.
2. Select one of the following options:

   The Default Credentials for All Repositories

   Submits the credentials that you used to log in to CA OM Web Viewer to each repository you try to access.

   The Individual Credentials for Each Repository

   Submits different credentials to different repositories. Typically, you do *not* need to supply separate credentials for each system. However, in certain circumstances your System Administrator can require you to change these values. All individual credentials match your login credentials by default.
3. Perform the following steps to locate your repository:
   - Locate the row of the repository that you want to change the credentials:

     To find other Repository objects, use the navigation arrows.
   - Sort the repositories.

     Click the Name column header or use the arrows for sorting. You can sort alphabetically or can reverse alphabetically.
4. Once you locate your Repository:
   - Replace the current user id.
   - Replace the current password.

     If you are a first-time user of Web Viewer, all the password fields are the same as your Web Viewer login password.
5. Click Update near the top right of the pane.

   The Credentials defaults are updated.

Restore Your Credentials

You can restore your repository credentials to the credentials that you used to log in to CA OM Web Viewer.

Follow these steps:

1. From the Configuration Tab, click the Credentials link in the left pane.
2. Select Individual Credentials for Each Repository.

3. To locate your repository, complete one of the following tasks:
   - Locate the row of the Repository you want to change the credentials for.

     Use the navigation arrows for finding other repository objects.
   - Sort the repositories.

     Click the Name column header or use the arrows for sorting the Repository Objects by name. You can sort alphabetically or can reverse alphabetically.
4. Click the checkbox to the left of that repository.
5. Click Restore credentials.

   The credentials of the repository now match your CA OM Web Viewer login credentials.
6. Click Update at the top right corner of the pane.

   The credentials for the chosen repository are restored.

Chapter 5: Frequently Asked Questions

This section presents some of the Frequently Asked Questions (FAQs) that help getting started with the product.

This section contains the following topics:

FAQs (see page 133)

FAQs

Which of the documents can I access?

The administrator determines which documents (or parts of documents) you can access. The Report List displays information about the reports to which you have access. To limit the display to those documents of interest, customize the Report List using date, report id filters with changing mode, recipient, or mail code.

Note: The administrator must know about the repositories that are in use. They must be able to set up, or request someone to set up, the infrastructure (CA DRAS for the mainframe) for web access.

Cross-report Indexes, Indexes, and Logical Views allow viewing of sections of one or multiple CA View documents. You can use indexes and logical views to view sections of one or multiple CA Bundl documents.

You can view text reports and reports in the following formats (provided you have the associated viewers or source applications on your PC):

- AFP reports
- CA Bundl reports
- CA Dispatch reports
- CA View reports
- Other PC application files

Note: CA OM Web Viewer does not support Xerox format, therefore, we suggest that you convert these documents to PDF files.

Where do the documents reside?

CA Output Management Web Viewer provides easy access to documents that reside on a mainframe. The data is not stored on your computer. The document resides in the product database; therefore, you can view the document on your PC.

How can I use the document data?

CA Output Management Web Viewer lets you email and save any type of document. CA OM Web Viewer also enables you to view, print, and export text documents. You cannot edit an original document but you can save a copy of any document on your PC. You can also save documents that the PC applications create (for example, Microsoft Word files and Microsoft Excel spreadsheets) by invoking the associated application.

Do I have to install CA Output Management Web Viewer on my primary Java web server?

Yes. CA Output Management Web Viewer must be running on the same server as the Java web server.

To update users or repositories, do I have to log in to the CA Output Management Web Viewer computer?

Yes. CA Output Management Web Viewer administration tools are integrated as a part of the web application. Log in to CA OM Web Viewer to make updates.

What are the prerequisites to implement cooperative processing using CA DRAS?

See the *Installation Guide* for prerequisites to use CA DRAS to implement cooperative processing with CA Output Management Web Viewer.

To run CA Output Management Web Viewer, do I need a database server?

CA Output Management Web Viewer stores the user ID and repository information in a JDBC-compliant database. You can also choose to use an embedded database that CA OM Web Viewer automatically deployed instead of an external one.

Important! The embedded database is a component that belongs to the installed CA OM Web Viewer application. If the embedded database with application level internal configuration is created under the application working folder, undeploying or uninstalling CA OM Web Viewer removes the embedded database. This situation is applicable on some application servers such as Tomcat.

We recommend that you use an external database or system level external configuration, so the administrative data is not affected by undeploying/uninstalling or redeploying/re-installing CA Output Management Web Viewer.

The deployment consideration when using WebSphere

If you selected to produce an EAR file during the installation, you can deploy this EAR file on WebSphere without additional settings. If you selected to produce the WAR files, set the class loader order to *Classes loaded with local class loader first (parent last)* in WebSphere for both application level and module level.

In addition, when redeploying an application on WebSphere, remove those compiled class files remaining from the previous installation. Those files can be located under the temp folder:

WebSphere/AppServer/profiles/AppSrv01/temp/ServerNode01/server1

How can I change the port number of the bundled Apache Tomcat server?

Find the file apache-tomcat/conf/server.xml and edit it in ASCII mode.

To change the port number, find the following line and change the setting. The string *8080* can be different if you specified another number during the installation.

<Connector port="8080">

To change the shutdown port, find the following line in the same file and change the port number. If you want to turn off the shutdown daemon, you can set the port number to *-1*.

<Server port="8005" shutdown="SHUTDOWN">

Does CA OM Web Viewer use the system temp folder at runtime?

No. Web Viewer does not use the system temp folder at runtime.

The CA OM Web Viewer is a Java EE application. CA OM Web Viewer can use the temp folder that is designated by the application server to which Web Viewer is deployed.

How can I be sure that a User role is updated?

To change the login role, be sure to use the Configuration tab.

Does the performance of CA OM Web Viewer benefit from the use of HiperSockets?

CA OM Web Viewer can see some benefit assuming HiperSockets are properly configured.

What is the initial database file size required for the database setup for CA OM Web Viewer?

No specific data file size for the database that is needed for CA OM Web Viewer in various database systems. The size depends on how many repositories, roles, and users would be set up and managed in the CA OM Web Viewer system. 10 MB of table space hold 100 repositories, 50 roles, and 1000 users, not including the audit log records that go into the database.

Why does the Print Preview button not appear in Internet Explorer?

To make the Print Preview button visible in Internet Explorer, see the instructions in the *Installation Guide*.

Why am I sometimes prompted for login credentials when I access reports or repositories?

By default, CA OM Web Viewer uses your CA OM Web Viewer login credentials as your credentials to all repositories. To access reports or repositories, mainframe credentials are required. If your credentials become invalid at runtime, CA OM Web Viewer prompts you for new credentials to attempt another connection.

For mainframe security reasons, your account can be suspended after a specified number of unsuccessful connection attempts with invalid credentials. The number is specified by your security administrator.

What are browser add-ons?

Browser add-ons are small executable programs that enable a web site to provide functionality beyond what the web browser can normally do. Web Viewer provides a browser add-on (ActiveX for Microsoft Internet Explorer and Extension/Plugin for Mozilla Firefox) for enhanced report printing and email integration. It is critical to note that the add-ons are executed on the client side (your workstation) and not on the web server (where Web Viewer executes).

Browser add-ons can be blocked from the installation or execution by browser settings, internet settings, and/or the Windows policies (set by your Windows administrator). The Web Viewer administrator can further restrict (disable) use of the add-ons for site-specific reasons.

What is the difference between web browser printing and browser add-on printing?

The web browser printing offers universal print support without the need of additional software installed on the client workstation. However, it does have some limitations.

The Web Viewer browser add-on for print offers enhanced printing. In particular, it has a fit-to-page option. It also presents important printer settings such as orientation and copies directly to the user rather than through secondary (optional) dialogs. The drawback of the add-ons is that they are limited to Internet Explorer and Mozilla Firefox on Windows only. Also, installation and/or execution can be blocked by browser settings, internet settings, and/or the Windows policies (set by your Windows administrator).

What is the difference between web-based email and browser add-on email?

The web-based email interface offers universal support without the need of additional software installed on the client workstation. However, this requires an SMTP (Simple Mail Transport Protocol) server to perform the message send operation. Also, end-users lack access to email features such as an address book and rich text message editing.

The Web Viewer browser add-on for email offers full integration with your installed email client application. This means, among other features, access to your address book and rich text message editing. The drawback of the add-on is that they are limited to Internet Explorer and Mozilla Firefox on Windows only. This is also limited to email client applications that provide MAPI32 support such as Microsoft Outlook and Lotus Notes. Finally, installation and/or execution can be blocked by browser settings, internet settings, and/or the Windows policies (set by your Windows administrator).

How do I install the browser add-ons?

The Web Viewer browser add-ons are typically installed when the web browser executes part of a web page that specifies the add-on should be used (print or email). The web browser then checks if the add-on is already installed. If it is not installed, the browser initiates a download of the add-on from the web server to the workstation.

Depending on your browser settings, you can be prompted to install the add-on. After installation, the web browser typically must be restarted to use the add-on.

Under certain conditions, a site can push the software to workstations. This is typically done for locked down environments where the installation using the web browser can be blocked.

How do I update the browser add-on?

For Microsoft Internet Explorer, the update occurs automatically if a newer version is available.

For Mozilla Firefox, there is no automatic update. If a newer version is available, uninstall the current version then install the new version.

How to I remove the browser add-ons?

Microsoft Internet Explorer:

1. Select Manage add-ons from Internet Explorer's Tools pull-down.
2. From the Manage Add-ons dialog, under the Show dropdown box, select All add-ons. Locate "UOMWV_Helper Control" (under "CA, Inc."), right-click it, then select More Information.
3. On the More Information dialog, click the Remove button.
4. Recommend restarting Internet Explorer to complete the action.

Microsoft Internet Explorer (alternative):

1. Locate the "Downloaded Program Files" folder under "Windows".
2. Open a command prompt (CMD.EXE) with "Downloaded Program Files" as the current folder.
3. Issue command: regsvr32 /u ERMHelper2AX.ocx
4. Expect confirmation dialog stating success.
5. Delete files ERMHelper2AX.ocx and ERMHelper2AX.inf.

Mozilla Firefox:

1. Select Add-ons from Firefox's Menu pull-down.
2. Select Extensions from the Add-ons Manager (tab).
3. Locate "CA OM Web Viewer Control 12.1.n.n" (your version can differ).
4. Click the Remove button.
5. Restart Firefox to complete the action.

Why do browser add-ons have Certificates?

Since the browser add-ons can be downloaded from virtually any web site, there must be some way to distinguish malicious versions from those add-ons that have been produced honestly. Sincere vendors purchase Certificates from a trusted source, like Verisign. The producer of the add-on incorporates the Certificate into the module. Therefore, the web browser can check the add-on (or add-on packaging) to determine if it is safe to download and/or execute. The browser has settings which can allow or inhibit these add-ons from being downloaded or executed.

Why can browser add-ons be blocked from installation or execution?

Each new release of a web browser is usually more secure than the prior release. Browser add-ons are often a method that malicious individuals can use to circumvent browser security. To address this issue, web browsers place many hurdles for installing add-ons, with default settings that often block installation or execution.

As an example, refer to: *MSDN Blogs: IEBlog: Internet Explorer begins blocking the out-of-date ActiveX controls* (August 2014).

Web Viewer provides a safe (nonmalicious) and signed add-on for both Internet Explorer (ActiveX) and Mozilla Firefox (Extension/Plugin).

The browser add-on is blocked. What can I do?

Microsoft Internet Explorer:

- Check the browser settings to allow (Enable) Signed ActiveX Controls to Download and Run (two different settings). Considering adding the Web Viewer web server to the "Trusted sites" under Internet Options, Security. Also verify that the user has Admin rights which are required to register the Control.
- For the sites that keep the browsers at their highest security settings, it can be necessary to push the add-ons to workstations using software delivery (bypassing the browser settings). For Internet Explorer, refer to the *Microsoft Internet Explorer: Library: Internet Explorer 11 (IE11) - Deployment Guide for IT Pros: ActiveX installation using group policy*. You can also contact CA support to get the requirements for the software push script.

Index

A

Add a Repository to a Role • 41
Add or Remove Favorites in a Subscription • 74
Add Owner Roles to a Repository • 14
Add Users to a Role • 43
Administering • 11
Administration Overview • 11
Assign a Subscription to a Role - Overview • 75
Assign Subscriptions to a Role • 47
Assigning Repositories to Roles - Overview • 40
Assigning Users to Roles • 42
Audience • 9
Auto Enrollment • 37
Auto Enrollment External Security EXIT Users • 56
Auto Enrollment LDAP Users • 52
Auto Enrollment Mainframe Users • 49

C

CA Output Management Web Viewer Single Sign On • 49
CA Technologies Product References • 3
Change User Roles • 127
Choose a Repository • 128
Configure Report Browsing • 124
Configuring • 111
Connect a Subscription to a User Role • 78
Contact CA Technologies • 3
Create a Directory Object • 65
Create a Repository Object • 13
Create a Role • 33
Create a Subrole • 34
Create a Subscription Using Favorites • 73
Creating a New Profile Object • 57
Creating a New User Object • 63
Customize the Filter Options • 18
Customize the Layouts • 24
Customize the Report Actions • 21
Customizing Role Settings • 39

D

Delete a Subscription • 75
Delete a Subscription from a Role • 78
DRAS Load Balancing • 25

E

Edit Favorite Properties • 71
Edit Role Properties • 35
eMail Type • 125
eMail Types • 92
Emailing File Options • 90
Enable or Disable Report Actions • 45
Export Admin Objects • 100
Exporting and Importing Admin Settings • 99
External Security EXIT • 53
External Security EXIT Authentication • 55

F

FAQs • 133
Favorite Properties • 70
Favorite Types • 68
File Saving • 94
Finding a User in the User List • 64
Frequently Asked Questions • 133

H

How CA OM Web Viewer Uses Roles • 29
How Role Hierarchies Work • 30
How Subscriptions Are Displayed • 79
How to Customize a Repository Object • 17

I

Import Admin Objects • 101
Import CA Output Management r11.5 Update • 102
Import Users • 102

L

LDAP Authentication • 50
LDAP Directory • 37
LDAP Distinguished Name Setup and Usage • 67
LDAP User Generation • 53
Listing Profile Objects • 58

M

Mainframe Authentication • 49
Managing Directory Objects • 64
Managing Preferences • 80

Managing Profile Objects • 56
Managing Repository Objects • 12
Managing Role Objects • 26
Managing Subscriptions • 68
Managing the After Login Settings • 127
Managing the Default Repository Filter Settings • 111
Managing the Favorites List Display Settings • 120
Managing the Report Level Actions Settings • 123
Managing the Report List Display Settings • 117
Managing User Authentication • 48
Managing User Objects • 60
Managing Your Credentials • 130

O

Override Favorite List Layout Settings • 123
Override Report List Layout Settings • 119
Overview • 9

P

Printing Properties • 88
Profile • 37
Profile Security and Auditing • 59

R

Remove Repositories from a Role • 42
Remove Subscriptions from a Role • 48
Remove Users from a Role • 44
Report Actions from the Subscription List • 79
Report Subscriptions in Roles • 46
Restore Your Credentials • 131
Role Authentication • 36
Role Hierarchy Example • 31

S

Security System Checking Order for Mainframe and LDAP Authentications • 54
Set the Default and Individual Credentials for Repositories • 131
Set the Login and Logout Settings • 83
Set the Maximum Pages Per Search Settings • 82
Set the Timeout Settings • 81
Setting Auditing Preferences • 96
Setting Display Preferences • 85
Setting General Preferences • 80
Setting Output Defaults • 87
Setting the Role Authentication Method • 37
Show Advanced Option for Favorites • 122
Show Advanced Options • 119
Show Repository List • 129
SMTP Email Account • 125
Specifying Permission to Designate Favorite Reports • 46
Statistics • 99

U

Understanding Report Access • 15
Understanding Role Types • 31
Update Date and Version Criteria • 112
Update Index Criteria • 115
Update Report Criteria • 114
Update the Favorite List Layout • 120
Update the Report List Layout • 117
User Object Properties • 61
Using AFP Transform • 25
Using Owner Roles with Repositories - Overview • 15

V

View the Roles in Your System • 33
Viewing Admin Info • 104
Viewing Auditing Preferences • 98
Viewing the Audit Log • 107
Viewing the Repository Status • 105
Viewing the User Status • 107
Viewing Web Statistics • 103