CA Embedded Entitlements Manager

Online Help

r8.4

Contact CA

Contact Technical Support

For online technical assistance and a complete list of locations, primary service hours, and telephone numbers, contact Technical Support at http://ca.com/support.

Provide Feedback

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

If you would like to provide feedback about CA product documentation, please complete our short customer survey, which is also available on the CA Support website.

CA Product References

This document references the following CA products:

- CA® Embedded Entitlements Manager (CA EEM)
- CA® Directory
- CA® SiteMinder® Web Access Manager (CA SiteMinder)
- CA® Identity Manager
- CA® Security Command Center
- CA® Integrated Threat Management
- CA® Enterprise Log Manager

Contents

Chapter 1: Introduction

CA Embedded Entitlements Manager (CA EEM) offers a common, shared approach to manage identities and access policies.

This web-based administrative interface lets you manage identities and access policies, and change the configuration of the CA EEM Server.

Chapter 2: Login

The Login page attaches a user to the CA EEM Server in the context of an application instance.

Note: To attach, the user must have rights to read the ApplicationInstance object as defined in the Policy page.

To login and attach, complete the fields, and then click Log In.

The user name and password are authenticated against the configured Global User/Global Groups source.

Login Page

The following fields appear on the Login page:

Application

Specifies the application instance to attach. Select <Global> to attach to the global application space.

User Name

Specifies the user name to login. You can use the user name EiamAdmin, which has global administrative privileges.

Note: The EiamAdmin user password is specified during the installation of CA EEM Server.

Password

Specifies the password for the selected user.

Remember my settings

Saves the field values (except for the password field) and displays them the next time when you launch the login page.

Chapter 3: Home

The CA EEM Quick Start menu lets you perform the following tasks:

- Manage Identities (see page 17)
- Manage Access Policies (see page 27)
- Manage Reports (see page 47)
- Configure (see page 83)
- Access Online Help

In addition, if the global users are stored in the CA-MDB (internal), and you are logged on as a regular user (not the EiamAdmin administrator), you can perform the following Self-Administration tasks:

- Change Password (see page 14)
- Unlock User (see page 15)

Change Password

The Change Password page lets you change your password. You can change your password to comply with a site security policy that requires you to change your password every 30 days or if you think your password has been compromised.

You can only change your password if the following conditions are matched:

- You are not attached as EiamAdmin
- CA EEM is configured with internal global users
- You correctly enter your old password
- You correctly confirm your new password
- Your new password meets the password policies defined on the Configure page

The following fields appear on this page:

Old password

Specifies the password you used to log in to the CA EEM Server.

New password

Specifies the new password you want to use.

Confirm password

Re-enter the new password.

OK

Changes your password if the new password meets the password policies.

Cancel

Returns to the home page without changing the password.

Unlock User

The Unlock User page lets you unlock disabled accounts. If a user has locked the account by entering wrong password too many times, you can unlock the user account for the user to access the application.

You can only unlock a user account if the following conditions are matched:

- CA EEM is configured with internal global users
- You correctly enter the account name and current password

The following fields appear on this page:

Username

Specifies the username of the account you want to unlock.

Password

Specifies the user's password.

Unlock

Unlocks the entered user's account. If the username is valid and the password matches, the account is unlocked.

Note: The user of the unlocked account must change their password at the next login to the web user interface.

Cancel

Returns to the home page.

Chapter 4: Manage Identities

Identities are users or group of users that you permit access to applications and their resources.

The Manage Identities tab contains the pages that let you list, search, view, and maintain global users, application instance-specific user details, global user groups, and application-instance specific user groups.

You can choose to manage the following:

Users (see page 18)

Lets you search, view, or maintain global users and application-specific user details, including modifying group membership.

Users in CA EEM are classified as follows:

Global users

Global users are users that are available for sharing across all application instances registered with CA EEM. Every user in CA EEM is a global user by default.

Application-specific users

Application users are specific to the application instance. The application-specific users are not shared across other application instances. Application-specific user attributes are defined when creating an application instance.

Groups (see page 22)

Lets you search, view, or maintain global user groups and application-instance specific user groups.

Groups in CA EEM are classified as follows:

Global user groups

Global user groups are groups that are available for sharing across all application instances registered with CA EEM.

Application-specific groups

Application-specific groups are specific to the application instance. The application-specific groups are not shared across other application instances.

Users

The Users tab lets you search, view, and maintain, global users and application-specific user details, including modifying group membership.

To search and list users from global users and application-instance specific user details

1. Select Global Users or Application User Details in the Search Users panel:

   - Select Global Users, if you want to search for users irrespective of application.
   - Select Application User Details, if you want to search for users of a particular application.

   The Search Users pane appears.

2. Enter your search criteria and click Go.

   List of users you have the right to view (read rights of GlobalUser and User) appear in the Users Panel.

   Note: You can select Show empty folders to list folders without any users.

   You can select a user from the Users panel to view, edit, change group membership, or delete the user.

Search Users Panel

The following fields appear on the Search Users panel:

Global Users

Includes all the users assigned to all applications.

Application User Details

Includes all the users assigned to a particular application.

Attribute

Specifies the attribute to search for. The Global User attributes are pre-defined. The Application User Detail attributes are defined for each application.

Operator

Specifies the operator to use for the search.

Value

Specifies the value to search for. You can use an asterisk (*) as a wild card when positioned as the first or last character only.

Leaving the Value field empty is the equivalent of setting it to *, which matches all values.

Note: If you are using CA SiteMinder as a user store or policy store, you cannot use the asterisk (*) as a wildcard to retrieve all groups.

Show Empty Folders

Searches for folders that are empty or without any user.

Go

Searches for users based on the criteria specified. The users appear under the Users panel.

Users Panel

The following fields appear on the Users panel:

New User

Displays the New User dialog, setting the user's folder to the one next to the icon.

Folder

Shows or hides the objects contained in the specified folder.

User Page

The User page lets you view and maintain global users and application-specific user attributes. You can also use it to change global and application-specific user group membership.

The following restrictions apply:

- If attached as <Global> application (not through an application instance), you can insert, modify, and remove global user attributes.
- If attached through an application instance, you can view and maintain user attributes for that application instance.
- You can only modify users if you have been granted rights to do so on the Policy page (write rights of GlobalUser and User).
- You also require rights to each modified user group (write rights of GlobalUserGroup and UserGroup). Groups are considered modified when you add or remove a user them from.

The following buttons appear on the Users page:

Save

Saves the application-specific user attributes and global user changes.

Delete

Removes the application-specific user attributes and global user object.

Close

Closes user object without saving.

The following fields appear on the Users page:

Folder

Displays the name of the folder into which this user is stored.

Name

Indicates the name of the user.

Note: Use only alphanumeric characters to prevent display problems.

The following fields appear in the [Application] User Details panel:

[application-specific]

Displays any user attributes defined in the application object.

User Groups

Indicates application-specific user groups to which this user belongs.

Global Groups

Indicates global user groups to which this user belongs.

Note: To display global user groups, complete the Search dialog and click Search.

The following fields only appear if CA EEM is configured to save global users internally:

Incorrect Login Count

Indicates the number of concurrent unsuccessful login attempts. This value is reset to zero after a successful login.

Override Password Policy

Indicates whether to permit this user to have passwords that do not meet the password policy.

Suspended

Indicates that the user is suspended, and cannot login.

Change Password at Next Login

Indicates that the user must change their password on next successful login.

Enable Date

Indicates the date the user account is enabled. The user cannot login outside of enable and disable dates.

Disable Date

Indicates the date the user account is disabled. The user cannot login outside of enable and disable dates.

Reset Password

Launches prompts to reset the user's password.

Note: If you try to reset the password from the Users page, CA EEM does not check the password policies.

Extended Group Membership

Provides additional information about each user under the following sections:

Application Groups

Indicates all the application-specific groups to which the user belongs either directly or as a result of group hierarchies.

Global Groups

Indicates all user groups to which the user belongs either directly or as a result of group hierarchies.

Dynamic Groups

Indicates all application-specific dynamic groups to which the user belongs either directly or as a result of group hierarchies.

Groups

The Groups tab lets you to search, view, and maintain, global user groups and application-specific user groups.

To search and list users from global user groups and application-instance specific user groups

1. Select Show global groups, Show application groups, or both.
2. If you select Show global groups, enter your search criteria including Attribute, Operator, and Value.
3. Click Go.

   One of the following occurs:

   - If you selected only Show global groups, a list of user groups matching the criteria appears in the User Groups panel.
   - If you selected only Show application groups, a list of user groups appears in the User Groups panel.
   - If you selected Show global groups and Show application groups, a list of user groups for both the categories appears in the User Group Panel.

   Note: Only groups that you have the right to view are displayed (read rights of GlobalUserGroup and UserGroup).

   You can select a group from the User Groups panel to view, edit, or delete the group.

Search User Groups Panel

The following fields appear in the Search User Groups panel:

Show global groups

Check to display global groups in the search result.

Attribute

Accessible only when Show global groups is selected. Choose the attribute to search for. The Global User Group attributes are pre-defined.

Operator

Accessible only when Show global groups is selected. Choose the operator to use for the search.

Value

Accessible only when Show global groups is selected. Enter a value to search for. You can use the asterisk (*) as a wild card when positioned as the first or last character only.

Leaving the Value field empty is the equivalent of setting it to *, which matches all groups.

Note: If you are using CA SiteMinder as a user store or policy store, you cannot use the asterisk (*) as a wildcard to retrieve all groups.

Go

Searches for groups based on the criteria specified. The groups appear in the User Groups panel.

User Groups Panel

The following fields appear in the User Groups panel:

New Application User Group

Displays the New Application Group dialog.

New Global User Group

Displays the New Global User Group dialog.

Folder

Shows or hides the objects contained in the specified folder.

Application Group/Global Group Page

The Application Group and Global Group page lets you view and maintain application-specific user groups and global groups.

The following restrictions apply:

- If attached as <Global> (not through an application instance), you can view and maintain global user groups.
- If attached through an application instance, you can also view and maintain user groups for that application instance.
- You can only modify groups if you have been granted rights to do so on the Policy page (write rights of GlobalUserGroup and UserGroup).

The following buttons appear on the Application Group/Global Group page:

Save

Saves the user group.

Delete

Removes the user group.

Close

Closes the user group object without saving.

The following fields appear in the Global User Group panel:

Folder

Displays the name of the folder into which this group is stored.

Name

Specifies the name of the global user group.

Note: Use only alphanumeric characters to prevent display problems.

Description

Specifies the description of the global user group.

Available Global Groups

Specifies the global user groups that this group can join.

Note: To view global user groups, complete the Search dialog and click Search.

Selected Global Groups

Specifies the global user groups of which this group is a member.

The following fields appear in the User Group panel:

Name

Specifies the name of the application-specific user group.

Description

Specifies the description of the application-specific user group.

Available User Groups

Specifies the application-specific user groups that this group can join.

Selected User Groups

Specifies the application-specific user groups of which this group is a member.

Chapter 5: Manage Access Policies

Access policies are rules attached to users that define their rights to access a particular application or a group of applications. You can define policies for a particular time period by specifying the calendar. CA EEM determines whether policies apply to user by matching identities and resource classes.

The Manage Access Policies tab lets you list, search, view, and maintain access policies and calendars, and perform specific permission checks.

You can choose to manage the following:

Policies (see page 28)

Let you search, view, or administer access policies, including administrative scoping policies, event policies, and delegation policies.

Policies are sorted in the tree based on the policy type and the policy's resource class.

Policies appear under two panels:

- Explicit Grants
- Explicit Denies

Policies include:

- Access Policies
- Delegation Policies
- Dynamic User Group Policies
- Event Policies
- Obligation Policies
- Scoping Policies

Calendars (see page 39)

Let you search, view, or administer calendars so that you limit the times when policies are effective.

Permission Check (see page 43)

Lets you perform specific permission checks against the access policies so that you can determine the scope and effectiveness of your policies.

Policies

The Policies tab lets you to search, view, and maintain access policies. Policies are sorted in the tree based on the policy type and the policy's resource class.

All policies assigned to users will have grant and denial rights.

Policies include:

Access Policies

Policies that define the access rights of an identity (user or group of users) and allow or deny those identities access to application resources.

Delegation Policies

Policies that let users delegate their authority to another user.

Dynamic User Group Policies

Policies that define application-specific groups and their memberships based on rules.

Event Policies

Policies that are used to determine which events are delivered, and which ones are only coalesced into summaries. By using event policies, you can configure which events are reported on in detail.

Obligation Policies

Policies that return required actions to the application after an authorization check. Obligation policies are application-specific. The policies contain one or more obligation names and attributes. Your application can use obligation policies to control what actions it should perform when access is granted or denied. For example, the application might send an event, start a workflow process, or send an email.

Scoping Policies

Policies that limit administrator access to CA EEM objects such as policies, a calendar, and so on.

To search and list policies

1. Enter your search criteria in the Search Policies panel, and click Go.

   A list of polices that match the criteria appear in the Policies panel.

   Note: Only policies that you have the right to see are displayed (read rights of Policy).

2. Select a policy from the Policies panel to view, edit, or delete.

Search Policies Panel

The following fields appear in the Search Policies panel:

Show all policies

Shows all policies in the search result.

Show policies matching identity

Shows all policies that apply to a specific identity (user).

Show policies matching resource

Shows all policies that apply to a specific resource class and resource name.

Identity

Active only when Show policies matching identity is selected. Enter the identity (user account name). Only policies that apply to this identity are displayed.

Resource Class Name

Active only when Show policies matching resource is selected. Choose the resource class with which to limit the policy search.

Resource

Active only when Show policies matching resource is selected. Enter a resource name with which to limit the policy search. Leaving this field blank will return with no policies.

Go

Searches for policies based on the criteria specified. The policies appear under the Policies panel.

Explicit Grants

Explicit Grant is an access permission that permits the identities with the specified access rights to the specified resources when the policy evaluates to true.

The following fields appear in the Explicit Grants panel:

New Policies

Displays the New Policy dialog.

Folder

Shows or hides the objects contained in the specified folder.

Explicit Denies

Explicit Deny is an access permission that prevents the identities access rights to the specified resources when the policy evaluates true.

The following fields appear in the Explicit Denies panel:

New Policies

Displays the New Policy dialog.

Folder

Shows or hides the objects contained in the specified folder.

Policy Page

Use the Policy page to view and maintain access policies.

Note: You can only modify policies if you have been granted rights to do so (write rights of Policy).

The following buttons appear on the Policy page:

Save

Saves the policy.

Save As

Saves the policy with a new name.

Delete

Removes the policy.

Close

Closes the policy without saving.

The following fields appear in the Policy panel:

Name

Specifies the name of the policy.

Note: Use only alphanumeric characters to prevent display problems.

Description

Describes the policy. For example, you might want to specify the purpose of the policy, such as grant doctor's access to patient records.

Calendar

Specifies the calendar to be used during the match phase of policy evaluation. If no calendar is specified, all days and times match.

Resource Class Name

Specifies the name of the resource class for which the policy is defined.

Example: All the delegation policies will have the resource class name as safeDelegation and all obligation policies will have the resource class name as safeObligation. You can define new resource classes using the Application Instances (see page 85) page.

Explicit Deny

If selected, the policy explicitly denies the access specified in the policy and located on the Explicit Denies tab.

Disabled

If selected, the policy is disabled, and is not considered for the match phase.

Pre-Deployment

If selected, the policy is considered inactive and is not considered for permission check identities.

Type

Controls the Access Policy Configuration as follows:

- If set to Access Policy, the actions and filters apply to all listed resources.
- If set to Access Control List, each listed resource has its own actions and zero or one filter.
- If set to Identity Access Control List, the following occur:

- Actions are set to particular identities.
- A default rule which applies to all identities that are not in the list is created.
- Identity types are marked with icons (user, application groups, global groups, or dynamic groups).

Note: There is a simple list for the resources. There are no filters for this type of policy.

Identities Panel

Specifies a list of identities (users, user groups, and global user groups) to be used during the match phase of policy evaluation. If this list is empty, all identities match.

Type

Specifies the type of identity, such as User, Application Group, Global Group, or Dynamic Group.

After you make a selection, you can specify search criteria such as attribute, operator, and value and click Search to display a list of matching identities.

Enter Identities

Displays the list of matching identities.

Selected Identities

Displays the list of identities to which the policy applies.

Access Policy Configuration Panel (Access Policy)

The following fields appear in the Access Policy Configuration panel when Access Policy is selected:

Resources

Specifies a list of resources to use during the match phase of policy evaluation. You can use the asterisk (*) to designate wild card characters, but only at the beginning or the end of the resource name. Asterisks in the middle of the resource class name are treated as literals.

If this list is empty, all resource names match.

Actions

Specifies the actions to use during the match phase of policy evaluation. If no actions are selected, all actions match.

Filters

Specifies filters to use in the Evaluate Phase of the policy evaluation.

Access Policy Configuration Panel (Access Control List)

The following fields appear in the Access Policy Configuration panel when Access Control List is selected:

Resources

Specifies a resource to use during the evaluate phase of policy evaluation. This resource has its own associated actions and filter.

Actions

Specifies the actions the associated resource name applies to.

Treat Resource Names as Regular Expressions

If selected, all the resource names will be considered as regular expressions.

Example: If an identity has access to the resource `'J*'`, saved as regular expression, the identity can access all the resources that start with J such as, John, Jane, and so on.

Filters

Specifies the filter the associated resource name applies to.

Obligations Panel (Obligation Policy)

Note: CA EEM does not support deny obligation policies.

The following fields appear in the Obligations panel when SafeObligation is selected:

Name

Specifies the name of the predefined obligation. You define an obligation using the Configure tab.

Comment

Specifies information about the obligation, such as the purpose or function of the obligation.

Attributes

Specifies one or more predefined user, global user, group, or application attributes.

Add Attribute

Lets you specify additional attributes for the obligation.

Enter/Select Identities

To enter or search identities

1. Select the identity type as User, Application Group, Global Group, or Dynamic Group and enter the identity. Or, click Search Identities.

   The Attribute, Operator, and Value fields appear. The Search Identities link appears as Enter Identities.

2. Choose the type, attribute, operator, and enter a value. Click Search.

   The identity appears.

3. Select the identity and click the arrow.

   The identity is selected and appears in the Selected Identities box.

Filters

Filters can be used to create fine-grained policies. Filters are attached to access policies to limit the scope of the policy. CA EEM uses filters during the evaluation phase of the policy evaluation process.

Each filter consists of the following components:

- The connector to the previous filter (logic)
- The number of left parentheses before the expression
- A sub-expression, consisting of a left hand side value, and operator, and a right hand side value
- The number of right parentheses after the expression

More Information:

Filters Pane (see page 36)

Create Filter

You can create filter to match the identities. Following is a sample filter to match the first name.

To create filter

1. Click Add Filter.

   The Filters pane appears.

2. Select Logic, None.
3. Select the corresponding Left Parenthesis.
4. Select the following options from Left type/value:
   - Global user
   - User Name
5. Select the following options from Operator:
   - String
   - Equal
6. Select the following options from Right type/value
   - Value
   - John
7. Select the corresponding Right Parenthesis.
8. Click Save to save the filter.

   The following table shows the options that you can select for the sample filter:

Logic	Left Parenthesis	Left type/value	Operator	Right type/value	Right Parenthesis
(ignore)	(	Global user: User Name	String ==	Value: John	)

Filters Pane

The following fields appear in each filter:

Logic

The connector to the previous filter. Ignored for the first filter.

(and)

The number of left and right parentheses that surround the sub-expression.

Left type/value and Right type/value

The left and right sides of the sub-expression. Type can be any of the following:

global user

Set this side of the expression to the value of a specified global user attribute.

global user group

Set this side of the expression to the value of a specified global user group attribute.

user

Set this side of the expression to the value of a specified user attribute. This value list is configurable in the application instance.

user group

Set this side of the expression to the value of a specified user group attribute.

named attribute

Set this side of the expression to the value of a specified resource attribute (passed in with the authorization request). This value list is configurable in the application instance.

session

Set this side of the expression to the value of a specified session attribute. Enter the name of the session attribute in the value.

environment

Set this side of the expression to the value of a specified environment attribute. Enter the name of the environment attribute in the value.

request

Set this side of the expression to the value of a request attribute. Choose identity, action, resource, or when as the value.

value

Set this side of the expression to a specific value. Enter the value.

dynamic user group

Set this side of the expression to the name of a dynamic user group.

request time (when)

Set this side of the expression to the offset in minutes from the current request time. For example, "-360" means 10 hours before the current request, and "60" means one hour after the current request.

calculation

Set this side of the expression to an XML based formula to be performed during policy evaluation.

Add Filter

Adds another empty filter to the end of the list.

Remove 🗑

Removes the associated filter.

Show Calculation Editor

Displays the Calculation Editor so that you can manipulate attribute values before a comparison.

Calculation Editor

The Calculation Editor lets you manipulate attribute values before a filter comparison.

The following fields appear:

Type

Choose from the list of operation types, such as STRING.

Operation

Choose from the list of operations, such as PLUS or MINUS.

Add Val

Click to add a value type and value pair.

Add Calc

Click to add a nested calculation.

How Policies Are Evaluated

During an authorization check, policy evaluation occurs in two phases:

Match phase

All policies for the specified resource class are matched against the following fields: policy's identities, resource name, actions, and calendar. If any of these are empty, they are assumed to include all possible values.

Evaluation phase

Matching policies are further evaluated against their respective filters. If a matched policy has no filters, or if the policy filters evaluate to true, the policy is assumed to have granted access.

Policies are evaluated in the following process:

1. Check for explicit denies:
   a. Match for explicit denies.
   b. Evaluate matched policies.
   c. In case of an explicit deny, stop checking, and return a denied recommendation specifying the policy.
2. Check for explicit grants:
   a. Match for explicit grants policies.
   b. Evaluate matched policies.
   c. In case of an explicit grant, stop checking, and return a granted recommendation specifying the policy.
3. Check for delegated authority:
   a. Match/evaluate the delegated authority. For each delegator, find a grant with no explicit deny.
   b. For each delegator, repeat the check for explicit denies, and then check for explicit grants.
   c. If grants was returned by delegation, return a granted recommendation specifying the policy and the delegator chain.
4. Calculate obligations for this access check:
   a. Add the following attributes to the ones passed in the authorization call:
      - PolicyName, the name of the obligation policy that caused the response
      - DelegationChain, the name of the delegation chain returned
   b. Match and evaluate each SafeObligation as follows:
      - ResourceClass set to SafeObligation.

        - Resource name set to {action} + "/" + {original resource class} + "/" {original resource name}.
        - Action set to FulfillOnGrant (if the authorization results in a grant), or FulfillOnDeny (if the authorization results in a deny).

    c. For each matching or evaluating policy do the following:

        - Append each obligation to the authorization results.
        - Calculate the values of the obligation attributes and append them to the authorization results.

    Note: Applications must handle the obligations returned from an authorization check. The application should not grant or deny access until and unless the obligations could not be performed.

5. In case of no matches, return a denied recommendation.

Calendars

Use the Calendars tab to view and maintain calendars. You use calendars in access policies to limit the times that the policies are effective.

Note: Only calendars that you have the right to see (read rights of Calendar in the Scoping Policies) are displayed.

You can select a calendar and view, edit, or delete the calendar.

Calendars Panel

The following fields appear in the Calendars panel:

New Calendar 📅

Displays the New Calendar dialog.

Folder 📂

Shows or hides the objects contained in the specified folder.

Calendar Page

Use the Viewing/Administering Calendars page to view and maintain calendars. You can use calendars in access policies to control the times that the policies are enabled.

Note: You can only modify calendars if you have been granted rights to do so on the Policy page (write rights of Calendar).

The following buttons appear on the Calendar page:

Save

Saves the calendar.

Delete

Removes the calendar.

Close

Closes the calendar without saving.

The following fields appear in the Calendar panel:

Name

Specifies the name of the calendar.

Note: Use only alphanumeric characters to prevent display problems.

Description

Describes the calendar, such as its purpose.

Effective Start

Specifies the effective start time and date of this calendar. An empty effective start means the calendar is effective for any time before the effective stop date.

Effective Stop

Specifies the effective stop time and date of this calendar. An empty effective stop means the calendar will always be effective after the effective start date.

Include Time Blocks

Specifies a block of time that is included in this calendar.

Add Include Time Block

Adds an empty include time block to the calendar.

Exclude Time Blocks

Specifies a block of time that is excluded from this calendar.

Note: Exclude time blocks override included times.

Add Exclude Time Block

Add an empty exclude time block to the calendar.

Time Blocks

The following fields appear in each time block:

Name

Specifies the name of the time block.

Start time

Specifies the starting time for this time block. Time is in 24 hour notation.

Duration

Specifies the duration for this time block. The format is hours : minutes.

Note: The Start time plus Duration cannot exceed 24 hours.

Recurring time interval

Specifies the interval which this specified time block recurs during the day. The format is hours : minutes.

Week Day Mask

Specifies the selected week days for which this time block applies. Only dates falling on the week days selected apply to this time block.

Month Day Mask

Specifies selected days of the month for which this time block applies. Only dates falling on the days of the month selected apply to this time block.

Month Mask

Specifies selected months for which this time block applies. Only dates falling in the months selected apply to this time block.

Select all

Select all values in the week day, month day, or month mask.

Clear all

Clear all values in the week day, month day, or month mask.

How Calendars Are Evaluated

Calendars are evaluated during the match phase of policy evaluation (see How Polices Are Evaluated (see page 38) for more information on the phases of policy evaluation). Calendar evaluation occurs in three steps:

1. Ensure the calendar is active by checking the effective start and stop dates. Empty start or stop dates imply always active.
2. Accumulate all include time blocks, then remove all exclude time blocks from the calendar.

   Note: Exclude time blocks override include time blocks.
3. Evaluate the time, down to the minute accuracy. If the minute evaluates to included, the calendar applies.

Permission Check

Use the Permission Check tab to run ad-hoc queries against the defined access policies. This provides a convenient way to test the effectiveness, scope, and coverage of the defined access policies.

For example, you can consider a permission as a request:

"Can {identity} perform {action} against the resource of type {resource class} and of name {resource} [with the following attributes}] [at the {specified time}]?"

If the permission check is permitted, the access policy that granted access, and optionally the delegator of the permission, is displayed in the Permission Check Results panel.

The following fields appear in the Permission Check Parameters panel:

Display debug information

If selected, the debug information appears showing how an authorization was made.

Synchronize Cache

Synchronizes the Web user interface with the latest sets of policies and user attributes. Click this button to ensure that the latest data was loaded into the cache.

Resource Class

Specifies the resource class you want to check.

Action

Specifies the action you want to check.

Resource

Specifies the name of the resource you want to check.

Identity

Specifies the name of the identity (user account name) you want to check.

Add Attribute

Click the plus ⊕ to add named attribute to the permission check.

Attribute

Specifies the name of the named attribute.

Value

Enter the value of the named attribute.

Remove

Removes the attribute/value pair from the permission check.

When

Shows a date/time control for the time of the permission check. Specifying a value runs the permission check as if it were that time/date. Leaving this empty uses the current time/date.

Include pre-deployment policies with the following labels

Specifies if the pre-deployment policies must be considered for permission check.

Run Permission Check

Executes the permission check against the specified resource class, and display the results in the Permission Check Results panel.

The following fields appear in the Permission Check Results panel:

Display debug information

If selected, the debug information appears showing how an authorization was made.

Time of the check

Specifies the time the check was run, which may be different than the time used within the permission check (see "When" above and below).

Result

Specifies ALLOW or DENY

Policy

If the permission check resulted in ALLOW, this column contains the name of the access policy that granted the access.

Note: This might not be the only policy that grants access.

Delegator

If the permission check resulted in ALLOW, and access was granted because another user delegated their authority, this column contains the "delegator hierarchy" that granted the access.

Identity

Specifies the identity from the permission check.

Resource Class

Specifies the resource class from the permission check.

Resource

Specifies the resource name from the permission check.

Action

Specifies the action from the permission check.

When

Specifies the when time from the permission check.

Named Attributes

Specifies the name and value of the named attributes from the permission check.

Clear All

Clears all previous permission check results from the display.

Chapter 6: Manage Reports

CA EEM lets you generate and manage reports for events generated in CA EEM Server.

Each report consists of one or more query displays that show event information in graphic, table, or Event Viewer formats. You can refine the graphic views by clicking on query elements to filter the report view or drill down to event information.

The Event Viewer display shows detailed event information that you can also sort or filter further.

The Eiam Reports tag contains the following reports related to CA EEM:

Authorization failures

Displays the authorization denial records.

Latest events

Displays the CA EEM admin, runtime and coalesced events.

Latest user updates

Displays events that are generated by creating, modifying, or deleting users.

More information:

Event Viewer Tasks (see page 54)
View a Live Report (see page 52)
Configuration (see page 77)

Set Up CA EEM to Manage Reports

To view or create reports in CA EEM you must have an access policy to the CALM resource class.

To create an access policy to CALM resource class

1. Log in as EiamAdmin to the CALM application.

   The CA EEM home page appears.

   Note: Only the CALM application has the CALM resource class for which the access policy must be created.

2. Click Manage Access Policies, Explicit Grant, Access Policy, CALM.

   The New Access Policy page appears with Resource Class Name as CALM.

3. In the Identities pane, select the identities for which you want to grant access.

   The identity is added to the resource class.

4. In Access Policy Configuration pane, enter the Resources name and click Add Resource.

5. Set the required permissions.

   Create

   Specifies the user can create reports.

   Note: If you do not specify the create permission, the user can view the reports only.

6. Click Save.

   The policy creation confirmation message appears and the user will now be able to manage reports.

Live Reports

You can manage reports from any application that is registered with CA EEM.

Note: You must have access policy to view a live report.

To manage live reports

1. Log in to CA EEM.

   The CA EEM home page appears.

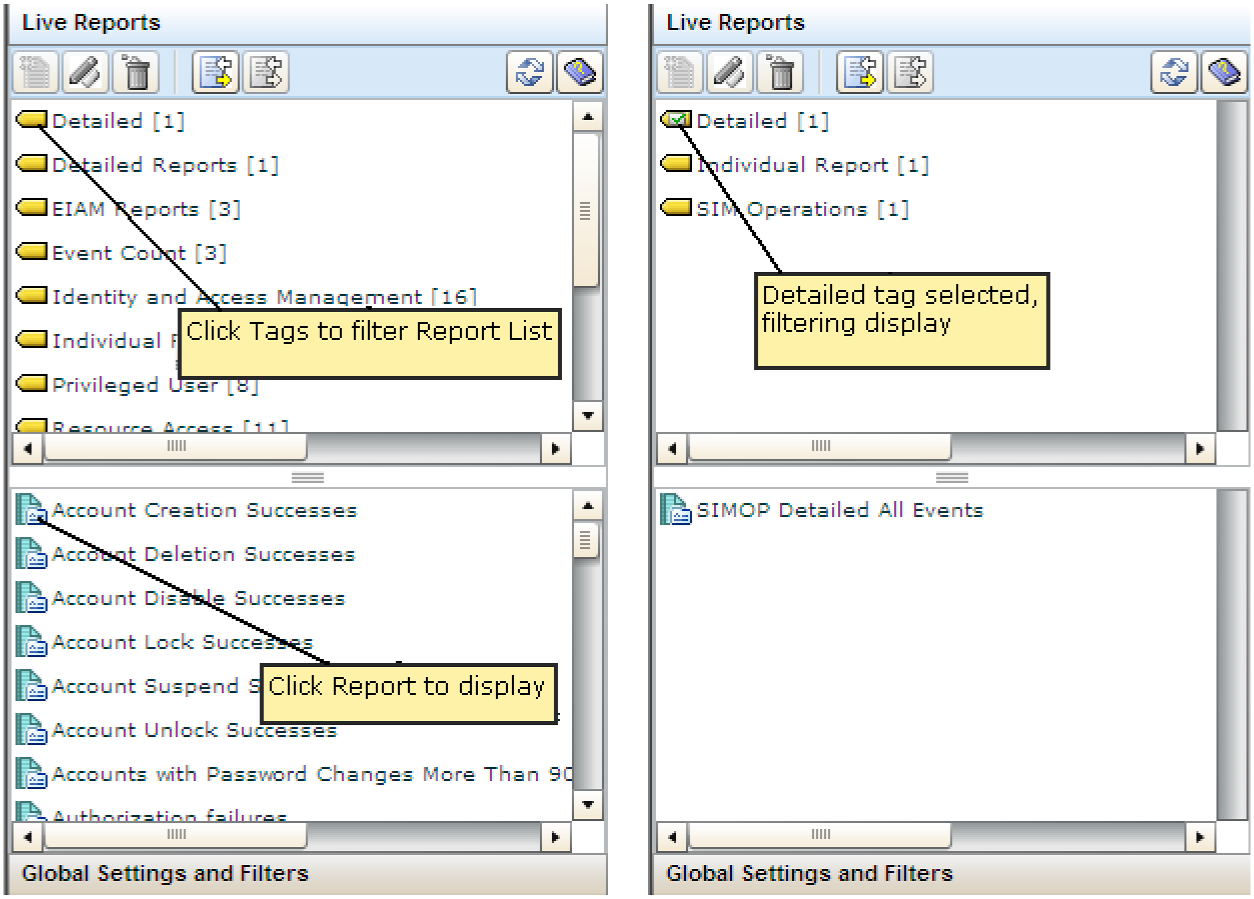
2. Click Manage Reports.

   The Reporting window appears, showing the live reports menu at the left side of the screen.

The menu pane is subdivided into a list of all report category tags with the number of reports in the category in brackets beside each, and a list of all the available individual reports in the Report List below it. Reports are displayed with a file card/report icon.

Selecting a category tag filters the display, showing other tags that share one or more reports with the selected tag, as well as the individual reports in that category. For example, selecting the Detailed category tag changes the display to show only Detailed, Individual Report, and SIM Operations in the tag area, and SIMOP - Detailed All Events in the individual reports area.

You can select multiple tags, narrowing the display accordingly. If you select additional tags, the number of available reports displayed changes along with the view.



Click Tags to filter Report List

Click Report to display

Detailed tag selected, filtering display

You can perform reports tasks including viewing, refining, and editing live reports from the details window.

Using Tags

Tags are an important part of the report functionality, allowing you to attach your reports and queries to categories for ease of reference, and providing an organizational framework for reporting on your environment. Report category tags also allow simple division of labor by role or type of event.

You can use the pre-defined tags or create your own custom tags for reports or queries. For example, you could create a "Monthly" tag to add to any reports you wanted to schedule every month for easy reference and viewing. This would also allow you to add or remove reports from the report jobs without editing the jobs themselves, by simply adding the Monthly tag to a new job, or removing it from an old one.

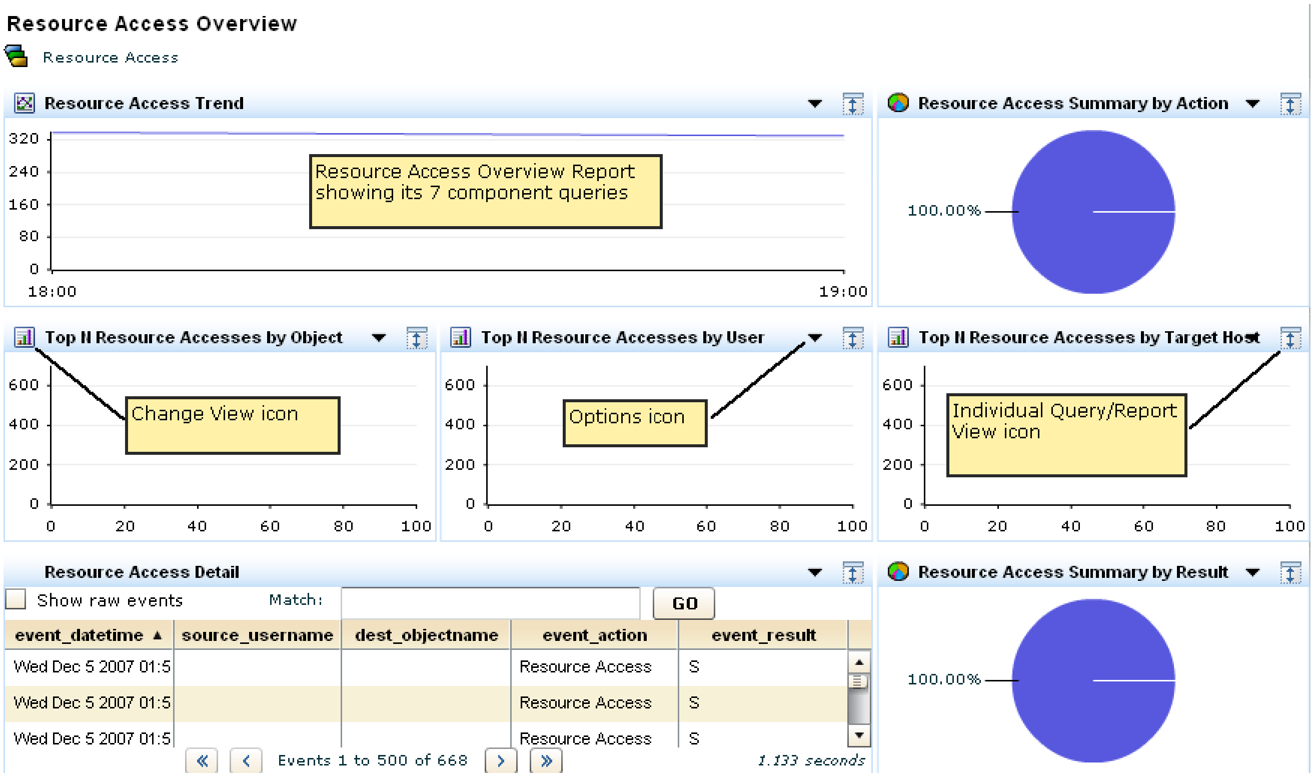
You add or remove tags for individual reports as part of the creation or editing process. Once you have added a new tag to a report, its title appears in the category pane of the Live Reports area, and clicking its associated check box will cause the reports containing that tag to appear in the area below. You can add new tags for queries in the same way you do for reports.

Note: We recommend that you plan carefully when creating new tags, since if you should later want to change or remove them, it must be done individually from all reports or queries which contain that tag.

View a Live Report

To view a live report, click its title in the report pane. The report you want appears in the details pane. Each report is a container which displays one or more specific query results in chart, table, or graphic form, as shown in the following illustration.

Note: You must have access policy to view a live report.



Resource Access Overview Report showing its 7 component queries

Change View icon

Options icon

Individual Query/Report View icon

Resource Access Overview
Resource Access
Resource Access Trend
320
240
160
80
0
18:00
19:00
Resource Access Summary by Action
100.00%
Top N Resource Accesses by Object
Top N Resource Accesses by User
Top N Resource Accesses by Target Host
600
400
200
0
0
20
40
60
80
100
Resource Access Detail
□ Show raw events
Match:
GO
Resource Access Summary by Result
100.00%

event_datetime ▲	source_username	dest_objectname	event_action	event_result
Wed Dec 5 2007 01:5			Resource Access	S
Wed Dec 5 2007 01:5			Resource Access	S
Wed Dec 5 2007 01:5			Resource Access	S

« ‹ Events 1 to 500 of 668 › » 1.133 seconds

You can view and refine report data in the query displays, and manipulate the queries themselves.

More information:

Create a New Report (see page 65)
Edit a Report (see page 64)

Display Local Filters

You can display local filters that are applied to your live reports from the Live Report details pane. Click the Show Local Filters icon at the top of the report pane to open the Local Filters dialog, which lets you review and edit or delete any current local filters.

Export a Live Report

You can export the report data and save it in XML format to use it any other formats.

To export a live report

1. Display the report you want to export.
2. Click Export to XML.

   A download location dialog appears.
3. Choose the download name and location you want, and click Save.

   The live report is saved.

Refine Live Report Graphic View

You can refine a live report from a query display, applying filters (see page 60), or drilling down to a related view of the event data.

To refine a live report view

1. Click on the chart element you want to refine.

   A popup menu displaying one or more of the following refinement options appears, depending on the query:

   Refine local by

   Displays a sub-menu containing one or more field values you can filter by. Choosing a field value creates a live report showing only those results that match your selected field value. The filter is local: it will not be applied to any other live report that you view.

   Refine global by

   Displays a sub-menu containing one or more field values you can filter by. Choosing a field value creates a live report showing only those results that match your selected field value. The filter is global: it will be applied to any other live report that you view, until edited or removed.

   Drill down to

   Displays a sub-menu containing one or more live reports you can display for additional information. Choosing a drilldown report displays it in the details pane, in place of the currently-selected report.
2. Select the type of filter and the field value you want to filter for, or the drilldown report you want to view.

   A live report with your chosen filter applied, or your chosen drilldown report appears.

Event Viewer Tasks

CA EEM displays certain event information in a table format called an Event Viewer. The Event Viewer format shares the structured data display of a table, but differs from a static table in that it is dynamic and allows a high degree of flexibility in presentation.

You can perform the following tasks in the Event Viewer:

- Search raw events using Matching
- Change the column order by dragging and dropping
- Show full events by selecting the Show raw events check box
- Open an event detail window by double clicking on an event row
- Refine Event Viewer displays
- Sort individual columns

Search Raw Events From the Event Viewer Display

You can search raw events from an event viewer query display. Each event consists of certain name/value pairs. Raw events are the event information (name/value pairs) contained in an event before it is mapped or parsed. This feature allows you to search all event information, including information that is not mapped.

To search raw events from the event viewer

1. Enter the value or values you want to filter by in the Match: field, using the appropriate match syntax (see page 55), and Click Go.

   The Event Viewer displays a raw events table, highlighting the value you entered, in any event fields where it occurs.

2. (Optional) Clear the Match: field, and Click Go.

   The Event Viewer displays its original results.

Match Syntax

You can use the Match function to search all event received information, including raw event information. Match searches raw event information (name/value pairs) contained in an event before it is mapped or parsed. This allows you to locate or search for specific event values even if they do not appear in refined events.

The Match function is accessible from various locations including Event Viewer (see page 54) queries, Global (see page 61) and Local (see page 63) Filter dialogs, and the Archive Query (see page 80) dialog.

You can search for single terms, or multiple terms using the syntax as outlined here:

Multiple Terms

You can enter multiple terms in the Match field; Doing so will return only those events containing *all* of the terms, since the Match syntax contains an implicit "AND" between multiple terms. For example:

```
user event
```

retrieves event information containing both user and event.

OR Queries

You can use the OR operator to search for either one of two terms. For example:

```
user OR event
```

retrieves event information containing either user or event. The OR operator takes precedence over the implicit AND between two adjacent terms. Thus, the query "user OR event source" returns events which contain either user or event and also source. Match does not provide any grouping operator, such as parentheses, to override this default precedence.

Note: OR must be capitalized.

Excluding Terms

You can use the - operator to exclude any events containing the term which follows it. For example:

```
user -event
```

retrieves event information containing user and *not* containing event.

A query must contain at least one non-excluded term, so the syntax:

```
-event
```

is invalid.

Phrase Searches

You can search for exact phrases by using the desired phrase in double quotes, for example:

"event source"

Wildcards

You can use the * character as a wildcard. For example:

on*

returns all event information including a term that starts with “on”. The wild card can only be used at the end of the term and NOT at the beginning. So

*on

is invalid.

Modify an Event Viewer Display

You can modify the Event Viewer display by removing or grouping columns.

To modify an Event Viewer display

1. Right-click in an Event Viewer column header.

   A menu appears presenting the following options:

   Hide column

   Removes the selected column from the Event Viewer display.

   Reset columns

   Returns all removed columns to the Event Viewer display.

2. Select the option you want.

   The Event Viewer display changes to reflect your chosen modification.

Refine an Event Viewer Display

You can refine a live report from an event viewer, applying filters (see page 60) to the display, or choosing to suppress or summarize events. You can also copy one or all events from the Event Viewer for pasting into a spreadsheet or other application.

To refine an Event Viewer display

1. Right-click in any Event Viewer column cell.

   A menu appears presenting the following options:

   Add to Local Filter

   > Adds a local filter to the query, using the value in the cell you right-clicked.

   Add to Global Filter

   > Adds a global filter using the value in the cell you right-clicked.

   Copy Event

   > Copies all the available event information in the Event Viewer row that you right-clicked to the clipboard for pasting. Pasting event details into Excel preserves the original row/detail structure.

   Copy All Events

   > Copies available event information from all the events displayed in the Event Viewer page to the clipboard for pasting. Pasting event details into Excel preserves the original row/detail structure.

2. Select the option you want.

   The Event Viewer display changes to reflect your filter choice, or copies the selected event information into the clipboard.

View Event Details

You can view event details and modify the Event Viewer display by opening the Event Viewer - Event Details window.

To view event details

1. Double-click anywhere in the Event Viewer display.

   The Event Viewer - Event Details window opens, showing all the event columns included in the Event Viewer with event details. Event columns set as visible (appearing in the Event Viewer) are selected in the Show check boxes.

2. (Optional) Select Hide Empty rows to remove all empty rows from the Event Viewer display.
3. (Optional) Clear the Show check box for any row you want to remove from the Event Viewer display, or select the Show check box for any row you want to add to the Event Viewer display
4. (Optional) Click the Copy button to copy the contents of the Event Details window to the clipboard. You can paste the event details into a text editor, or an Excel spreadsheet.

   Note: Pasting event details into Excel preserves the original row/detail structure.

Exporting and Importing Report Definitions

You can export and import details of reports for use in other CA EEM servers. This allows you to transfer successful reports to other servers, or from a test to a live environment.

Export Report Definitions

You can export the details of user-created files for use in other servers. The export is saved as an XML file.

To export report details

1. Click the Reports tab.

   The Report List appears.

2. Click the Export Details button at the top of the list.

   The Export User Definitions dialog appears, displaying available user-created reports.

3. Select the report or reports you want to export using the shuttle control, and click Export.

   An export dialog appears.

4. Enter or browse for the location you want to save the XML export files, and click Save.

   The Report files are saved to your chosen location and a confirmation dialog appears.

5. Click OK, and then Close.

   The Export User Report Definitions dialog closes.

Import Report Definitions

You can import report definition XML files for use in the local server.

To import report details

1. Click the Reports tab.

   The Report List appears.

2. Click the Import Definitions button at the top of the list.

   An Import File dialog opens

3. Enter or browse for the location of the file you want to import, and click OK.

   The Import Results window appears.

4. Click Import Another File to repeat step 3, or Close.

   The Import Results window closes.

Live Report Filters

You can set or edit live report filters to further refine the event information displayed in your reports. You can also add, edit or remove global filters from the main CA EEM window. You can also add local filters from the live reports Details pane, or from within an individual live report (see page 53) query.

There are two types of live report filters:

Global Filter

Applies to all live reports: Once created, a global filter will be applied to all live reports you view or add until you remove or modify it. A Global Filter will not be saved on logout.

Note: The Global Filter is set for the last 6 hours by default.

Local Filter

Applies only to the current live report. When you view a new report, the local filter will no longer be applied, nor will it be saved, unless you save the filtered live report as a favorite with that filter set.

Create a Global Filter

You can create a global filter to apply to all reports.

To create a global filter

1. Click the Global Filters icon at the top of the main window.

   The Global Filters and Settings dialog appears, displaying the Quick Filters tab.

2. (Optional) Specify the time period you want your filter to search, using the Time Range pull-down menu.
3. (Optional) Select the Match check box to enter a specific value by which you want to search all available raw events.

   Note: You can search for multiple values, phrases, or partial values in the raw events by using the specialized Match syntax.

4. Click Add Filter to specify event fields that you want to include in the filter.

   The Column pull-down menu and Value entry field appear.

5. Choose the event field you want to include in the filter, and enter the value that the field must have to be displayed in the filtered live reports. You can enter multiple event field names and values by clicking Add Filter again. Selecting the Exclude button includes every value *but* the one you enter for the chosen event field name.
6. (Optional) Click the Advanced Filters tab to add additional qualifiers.
7. (Optional) Click the Settings tab to choose settings for the query.
8. Click Save.

The Global Filters and Settings dialog closes, and the new filter is applied to live reports.

Edit a Global Filter

You can edit an existing Global Filter.

To edit a global filter

1. Click the Global Filters icon at the top of the main window.

   The Global Filters and Settings dialog appears, displaying the Quick Filters tab.

2. Change or add parameters as needed. You can remove an individual quick filter parameter by clicking the Delete icon beside it.

3. Click Save.

   The Global Filters and Settings dialog closes, and the edited filter is applied to live reports.

Remove a Global Filter

You can remove a Global Filter by removing its individual parameters, returning the live reports to their default unfiltered state.

To remove a global filter

1. Click the Global Filters icon at the top of the main window.

   The Global Filters and Settings dialog appears, displaying the Quick Filters tab.

2. Click Clear All, and then Save.

   The Global Filters and Settings dialog closes, and the filter is removed from live report views.

Create a Local Filter

You can create a local filter to narrow the scope of the live report you are currently viewing, or search raw events (the event information in its native pre-mapped format).

To create a local filter

1. Click the Reporting tab.

   The tab opens, displaying the Live Report and Global Settings and Filters bars.

2. Open the live report you want to filter, and click the Local Filters icon at the top of the Details pane.

   The Local Report Filters dialog appears, displaying the Quick Filters tab.

3. (Optional) Select the Match check box to enter a specific value by which you want to search all available raw events.

   Note: You can search for multiple values, phrases, or partial values in the raw events by using the specialized Match syntax.

4. Click Add Filter.
5. Choose the event field you want to include in the filter, and enter the value that the field must have to be displayed in the filtered live reports. You can enter multiple column values by clicking Add Filter again. Selecting the Exclude button includes every value *but* the one you enter for the chosen event field name.
6. (Optional) Click the Advanced Filters tab to add additional qualifiers.
7. Click Save.

The filter is applied to the live report display.

Edit a Local Filter

You can edit an existing local filter.

To edit a local filter

1. Click the Local Filters icon at the top of the Details pane.

   The Local Report Filters dialog appears, displaying the Quick Filters tab.

2. Change or add values as needed. You can remove individual filter settings by clicking the Delete icon beside each one, or remove a Match value by clearing the check box.
3. Click Save.

   The edited filter is applied to the live report display.

Remove a Local Filter

You can remove a Local Filter by removing its individual parameters, returning the live report to their default unfiltered state.

To remove a local filter

1. Click the Local Filters icon at the top of the Details pane.

   The Local Report Filters dialog appears, displaying the Quick Filters tab.

2. Click Clear All, and Save.

   The Local Report Filters dialog closes, and the local filter is removed from the display.

Edit a Report

You can edit a report in CA EEM.

To edit a report

1. Click the Reports tab.

   The Report List appears.

2. Select the report you want to edit, and click the Edit button at the top of the list.

   The Report Design wizard appears.

3. Make the changes you want, and click Save, or Save As to save a modified pre-defined report. See Create a New Report (see page 65) for information on specific parameters.

   Note: If you are editing a pre-defined report and have not changed the report name, you will receive a prompt asking if you want to change the report name.

   The edited report appears in the Report List.

Create a New Report

Note: To create a new report in CA EEM, you must have the necessary access permissions.

You can create a new report, setting which queries which you want to include, their placement in the report display, and the tags associated with the new report.

To create a new report

1. Click the Reports tab.

   The Report List appears.

2. Click the New Report button at the top of the Report List.

   The Report Design page appears.

3. Enter a report name. You may also enter optional description information for reference.
4. Add any existing tags (see page 51) you want to associate the report with, using the Tags shuttle control.
5. (Optional) You can also create and add a custom tag by entering a name, and clicking the Tag button below the shuttle control.
6. Select or enter the number of rows and columns you want to appear in your report, in the Report Layout pane. These settings control the number of query display areas the report will contain. You may include up to 10 rows and/or columns.

   The appropriate number of rows, columns, and query displays appears in the report layout pane.

   Note: You can use the arrows at the right side and bottom of individual query display areas to expand or shrink them horizontally or vertically as needed.

7. Drag the query you want to display in each display area from the Query Library to the appropriate area in the report layout.
8. (Optional) Click on the Edit button at the top of each query display area to edit the query you have placed there or create a new query (see page 67).
9. Click Finish.

   The Report Design dialog closes. The new report appears in the Report List.

More information:

View a Live Report (see page 52)
Using Tags (see page 51)

Delete a Report

You can delete report in CA EEM.

To delete a live report

1. Click the Reports tab.

   The Report List appears.

2. Select the report you want to delete, and click the Delete button at the top of the list.

   A confirmation dialog appears.

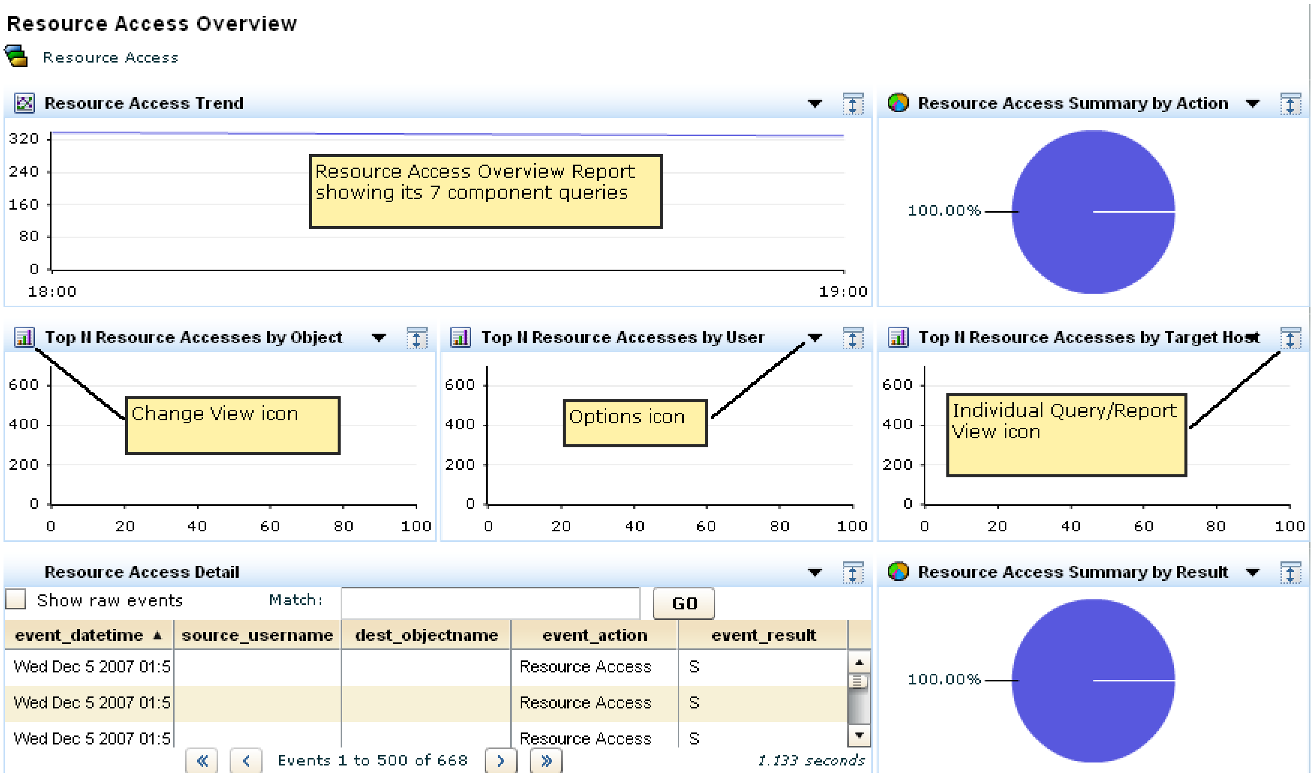
3. Click OK.

   The deleted report is removed from the Report Library.

Report Queries

Each report is composed of one or more query displays. Each one shows the results of a specific query of the event database in chart, table, or graphic form as shown in the following illustration.

Note: You must have access privileges to modify the queries.


Resource Access Overview
Resource Access
Resource Access Trend
320
240
160
80
0
18:00
19:00
Resource Access Summary by Action
100.00%
Top N Resource Accesses by Object
Top N Resource Accesses by User
Top N Resource Accesses by Target Host
600
400
200
0
0
20
40
60
80
100
Resource Access Detail
Resource Access Summary by Result
100.00%

Resource Access Overview Report showing its 7 component queries

Change View icon

Options icon

Individual Query/Report View icon

□ Show raw events   Match: GO

event_datetime ▲	source_username	dest_objectname	event_action	event_result
Wed Dec 5 2007 01:5			Resource Access	S
Wed Dec 5 2007 01:5			Resource Access	S
Wed Dec 5 2007 01:5			Resource Access	S

« ‹ Events 1 to 500 of 668 › »   *1.133 seconds*

You can perform various tasks at the individual query level, including altering the display type, and filtering or editing the query itself.

Creating a New Query

You can create new queries to include in your custom live reports. It involves the following main steps:

1. Adding Identity and tag details
2. Selecting query columns
3. (Optional) Setting query conditions and filters
4. Setting date range and result conditions
5. (Optional) Choosing visualization options for the query display
6. (Optional) Adding drilldown values for the query

Create a Query

To create a query, you must create the SQL statement that retrieves the event information you want from the event database.

To create a query

1. Click the Edit Report icon.

   The Report Design window appears.

2. (Optional) Enter the required details.
3. Click Layout.

   The Report Layout sub window appears.

4. Click the 'Edit Panel Contents' icon for the query in Report Layout.
5. Click Query Columns.
6. (Optional) Select either of the qualifying check boxes, Unique events only or Limit number of results. If you select Limit number of results, enter the maximum number of results you want in the number of results field.
7. Set the event attributes you want to include in the query by dragging them from the list of available attributes on the left into the Selected Columns pane. They will appear in the query display in the order in which they are entered.
8. (Optional) Select the settings you want for each column, including:

   Display Name

      Lets you enter a different name under which the column will appear. If you enter no Display Name, the native field name will appear, "event_count" for example.

Function

Lets you apply one of the following SQL functions to the column's values:

- AVG - returns the average of the event values.
- COUNT - returns the total number of events.
- SUM - returns the sum of the event values.
- MIN - returns the lowest event value.
- MAX - returns the highest event value.
- UNIQUECOUNT - returns the number of unique events.

Group Order

Sets the query display to show the selected columns grouped by the selected attribute. For example, you can set the query to group events by sourcename. You can control the order in which it is applied to various columns. If the first column values are identical, the second will be applied. For example, multiple events from the same source might be grouped by username.

Sort Order

Controls the order in which the selected value is sorted. You can control the order in which it is applied to various columns. If the first column values are identical, the second will be applied.

Descending

Sets the column values to display in descending order (highest to lowest value) rather than the default ascending order.

Not Null

Controls whether the column will be displayed if it contains no value. Selecting the Not Null check box removes the column from the query display if it is empty. The default value displays an empty column.

Visible

Controls whether the column is visible in the query display. You can use this setting to make the column data available in the details view without showing it in the display itself.

9. (Optional) Use the up and down arrows at the top of the Selected Columns pane to change the column order as needed.

10. Click the appropriate arrow to advance to the Query Design step you want to complete next, or click Save if you are finished.

    If you click Save, your new report appears in the Query Library, otherwise the Query Design step you choose appears.

Set Query Conditions

You can set conditions for your query by using the interface to build SQL language defining the events it returns.

To set query conditions

1. Click Query Conditions.
2. Select the Query Conditions check box for any of the specified field names you want to define, and enter the value you want.
3. Add Advanced Filters (see page 71) as needed.
4. Click the appropriate arrow to advance to the Query Design step you want to complete next, or click Save if you are finished.

   If you click Save, your new report appears in the Query Library, otherwise the Query Design step you choose appears.

Using Advance Filters

You can use SQL-based advanced filters to qualify any function that queries the event database, including narrowing queries, refining scheduled reports, or customizing quick filters. The Advanced Filters interface helps you create the appropriate filter syntax by providing a form for entering logics, columns, operators and values according to your filtering requirements.

Note: This section contains a brief overview of the SQL terms used in advanced filters. We recommend a full understanding of SQL, and the Common Event Grammar to use advanced filters to their full potential.

The following SQL logical terms join multiple filter statements.

And

Displays the event information if *all* the joined terms are true.

Or

Displays the event information if *any* of the joined terms are true.

The following SQL operators are used by advanced filters to create the basic conditions:

Relational Operators

Include the event information if the column bears the appropriate relation to the value you enter. The following relational operators are available:

- Equal to
- Not Equal to
- Less than
- Greater than
- Less than or equal to
- Greater than or equal to

For example, using *Greater than* would include the event information from your chosen column if its value is greater than the value you set.

Like

Includes the event information if the column contains a pattern you enter, using % to set the pattern you want. For example, L% would return any values beginning with L, %L% would return any values with L included as neither first nor last letter.

Not like

Includes the event information if the column does not contain the pattern you specify.

In set

Includes the event information if the column contains one or more of the values in the comma-separated set you enter.

Not in set

Includes the event information if the column does not contain any of the values in the comma-separated set you enter.

Matches

Includes any event information that matches one or more of the characters that you enter.

Create an Advanced Event Filter

Advanced filters are used by many features, including query creation, report scheduling, and local and global filters.

To create an advanced filter

1. Click the New Event Filter button.

   The first row of the event filter table becomes active, and its Logic and Operator columns are populated with the default values "And" and "Equal to" respectively.

2. (Optional) Double-click the Logic cell and change the logic value as needed.
3. Double-click the Column cell, and select the event information column you want from the pull-down menu.
4. Double-click the Operator cell, and select the operator you want from the pull-down menu.
5. Double-click the Value cell, and enter the value you want.
6. (Optional) Double-click the open and closed parentheses cells and enter the number of parentheses you need.
7. (Optional) Repeat steps 1 through 6 as needed to add additional filter statements.
8. Click Save when you have entered all the filter statements you want.

Set Result Conditions

You can set a date range and other result conditions for the query, including row limits and base display time period.

To set result conditions

1. Enter the date range selection you want. If you enter no date range, the query will be applied all events in the database.
2. Select any Results limits you want. Selecting Set limit to X rows lets you enter a maximum number of event rows. Selecting Use X for time granularity lets you choose the time period field you want from the pull-down menu.
3. Select any Result Conditions you want, including:

   Grouped Event conditions

   Search for various types grouped event conditions, the latest grouped event after a selected date, for example. A grouped event is a refined event for which you have set a Function and Group Order in the Query Creation (see page 67) step.

   Local Time Zone

   Displays the local time zone where the event occurred.
4. Click the appropriate arrow to advance to the Query Design step you want to complete next, or click Save if you are finished.

   If you click Save, your new report appears in the Query Library, otherwise the Query Design step you choose appears.

Create a Query Display Visualization

To create a new query display you must set the Visualization details, which control how the event information appears.

To create a query display visualization

1. Choose whether you want your query display to use an Event Viewer or Chart.
2. If you choose Event Viewer, the visualization step is complete. The event columns will appear in the Event Viewer display in the order in which you placed them during the Query Columns construction step.
3. If you choose a Chart, you can select one or more chart types. Selecting multiple chart types allows users to toggle back and forth between them in the report display. The up and down arrows that appear beside each type control the order in which they appear in the display's pull-down display menu, from top to bottom.

   Note: Table is always available as a chart type.
4. Select the event you want to appear as the X (horizontal) Axis from the column pull-down, enter label text if you want any to appear, and select one of the following options from the display type menu:
   - Category - Use this option for string or text value columns, such as source_username
   - Linear - Use this option for numeric values, such as event_count
   - Datetime - Use this option to display time values in the local date/time
   - Datetime_UTC - Use this option to display time values in GMT
5. Repeat Step 4 using the Y-Axis Settings menus to set the Y (vertical) Axis column, label, and type options.
6. Click the appropriate arrow to advance to the Query Design step you want to complete next, or click Save if you are finished.

   If you click Save, your new report appears in the Query Library, otherwise the Query Design step you choose appears.

Add a Drilldown Report

You can add one or more drilldown reports to your query, allowing the user to click a query display element and display another related report.

To add a drilldown report

1. Click the Add Drilldown button.

   The Drilldown selection dialog appears.

2. Enter the name, or browse for the live report you want to make available as a drilldown.
3. (Optional) Click Add Parameter to pre-set a local filter for the drilldown report.

   The Parameters pull-down menu appears.

4. Select the event column parameter you want to set as a local filter.
5. (Optional) Repeat step 3 to add additional parameters. The available parameters are limited to the event columns included in the native report.
6. Click the appropriate arrow to advance to the Query Design step you want to complete next, or click Save if you are finished.

   If you click Save, your new report appears in the Query Library, otherwise the Query Design step you choose appears.

Edit a Query

You can edit existing queries.

To edit a query

1. Select the query you want to edit, and click on the Edit button at the top of the Library pane.

   The Query Design wizard appears.

2. Make the changes you want, and click Save, or Save As to save a modified pre-defined query. See Create a New Report (see page 65) for information on specific parameters.

   Note: If you are using a pre-defined query as a template and have not changed the name, you will receive a prompt asking if you want to change its name.

   The edited query appears in the Query Library.

Delete a Query

You can delete a query.

To delete a query

1. Display the query you want to delete, and click on the Edit button at the top of the Library pane.

   The Edit Live Report dialog appears.

2. Click Delete.

   A confirmation dialog appears.

3. Click Yes.

   The deleted query is removed from the query library.

Alter the Query Display Type

You can view alternate display types for certain queries. The exact view types available are controlled by the creator's design choices of queries.

Event Viewer queries have no alternate views.

To alter the query display type

1. Click the Change View icon at the top left of the query display.

   A pop-up menu appears, displaying the available views.

2. Click the view you want.

The query display changes to the selected view.

Export a Query

You can export an individual query by saving the data displayed in XML format.

To export a query

1. Click the Options icon at the top right of the query display.

   A popup menu appears, displaying the options.

2. Click Export to XML.

   A download location dialog appears.

3. Choose the download name and location you want, and click Save.

   The query is saved in the specified location.

Set Query Display Result Conditions

You can change a query display's result conditions. This is different from the result conditions set during query creation in that it functions as a local filter, overriding the normal query settings for the current view only. Changing reports will remove any result conditions set from the query display.

To set query display result conditions

1. Click the Options icon at the top right of the query display.

   A popup menu appears, displaying the result conditions icon and other options.

2. Click the Result Conditions icon.

   The Result Conditions dialog appears.

3. Make any changes you want and click Save.

   The query is displayed using the new result conditions.

Maximize a Query Display

You can enlarge a query display to view additional detail.

To maximize a query display

1. Click the Query/Report View icon at the top right of the query display you want to maximize.

   The query you choose appears in an enlarged view, displaying the legend at the top left.

   Note: The legend does not appear in the default live report view.

2. (Optional) Select the other query tabs, if the live report contains more than one query, to shift from one maximized query view to another.

3. (Optional) Click the Query/Report View icon to return to the default live report view.

Configuration

The configuration page lets you set parameters for archiving and querying events, and for filtering archived files. It contains the following divisions to set the parameters:

Services (see page 77)

Archived events are stored in a database file whose location you can define. You can configure the archive settings based on the number of event entries or the number of days.

Archive Query (see page 80)

Use the Archive Query pane to view the events that are in the archived files by running a query from the Web interface.

Services

Use the Event Log Store (see page 77) pane under Services to configure archive settings.

Event Log Store

The event log store archive settings allow you to specify how often data is archived and where it is stored. Both active databases and archived event information are queried.

You can configure the following Event Log and archiving settings:

Database Directory

Specifies the location of the active event database, which is updated at the rate set by the Bulk Count and Bulk Timeout values.

Storage Directory

Specifies the location to move the data that has exceeded the maximum archived days.

Query Connections

Sets the maximum number of query threads permitted. Increasing the number of query threads speeds communication, but may have performance implications, as it uses more CPU resources.

Maximum Queries

Sets the maximum number of individual queries awaiting processing. Any excess native events are delayed at the source.

Bulk Count

Specifies the number of events that trigger a bulk insert. When this number of events is received or when the Bulk Timeout period elapses, whichever comes first, any received events are inserted into the database.

Bulk Timeout

Specifies the number of seconds after which a bulk insert is automatically triggered. When this period elapses or the Bulk Count reached, whichever comes first, any received events are inserted into the database.

Maximum Rows

Sets the maximum number of events your event database can contain. When the event count exceeds this value, the excess events are archived, oldest events first.

Note: By default, CA EEM archives events after every 100,000 events.

Max Archive Days

Specifies the number of days warm db files will be maintained in the archive directory. The warm db files will be converted to cold db files after the number of days they are maintained exceeds the Max Archive Days. After Max Archive Days, the warm db files will be deleted from the archive directory.

Export Policy

Specifies the number of hours defrost db files will be maintained in the archive directory. The defrost db files will be deleted after the specified Export Policy number of hours.

Self-Monitoring Events

Self-Monitoring events are logged for most of the user actions. These events allow you to track which actions have been taken and their success or failure. Self-monitoring events are displayed in Event Viewer format for each server, and can also be accessed as live reports using the SIMOP-Detailed Self Monitoring Events template.

All self-monitoring events fall into one of these categories:

System Access

Includes actions such as:

- Successful login
- Failed login

Operational Security

Includes actions such as:

- Starting or termination of the Reporter service
- Application errors caused by failed actions

Resource Access

Includes actions such as:

- Exporting a report or query
- Loading, annotating, or deleting a Generated Report

View a Self-Monitoring Event

You can view self-monitoring events for each server.

To view self-monitoring events

1. Click the Configuration tab.

   The Configuration pane appears.

2. Select Event Log Store

   The Event Log Store configuration pane appears.

3. Click the Self-Monitoring Events tab.

   The Self-Monitoring Events viewer pane appears. You can perform any of the normal reports tasks from the Self-Monitoring Events pane, including:

   - Event Viewer tasks
   - Global or Local filtering
   - Exporting
   - Editing

Archive Query

You can create queries to search archived event data, using quick or advanced filters. The query does not allow you to view the data, simply to determine its presence in the archive. If the data has been archived, and thus removed from the system, the query will inform you which files to restore to be able to temporarily report on the data again.

You can control the availability of archived event data that can be queried, using the Event Log Store (see page 77) settings from the Services pane.

More information:

Perform an Archive Query (see page 80)
Setting an Archive Query Quick Filter (see page 81)
Using Advanced Filters (see page 81)

Perform an Archive Query

You can perform an archive query to determine in which archive files the data you need resides. The Log Manager server must run long enough for the archive interval to pass before any archive files are created.

To perform an archive query

1. Log in to CA EEM.

   The CA EEM home page appears.

2. Click Manage Reports.

   The Reporting window appears, displaying the live reports menu at the left side of the screen.

3. Select the Configuration tab and select the Archive Query bar.
4. Provide Quick Filter information or select the Advanced Filters tab.

   Advanced filters allow you to more detailed search criteria in an SQL statement format using the CEG fields to which the events in the log store have been mapped.

5. Click Query to search the log file archive index.

   The query returns an archive file name, or a list of file names, that contain event data matching the search criteria you entered.

6. Restore the named files from the archives and run the desired Live Reports to obtain data.

Setting an Archive Query Quick Filter

You can set a quick filter to narrow your archive query.

To set an archive query quick filter

1. Select the Configuration tab.

   The tab opens, displaying the Archive Query and Services bars.

2. Click Archive Query.

   The Archive Query details pane opens, displaying the quick filter tab.

3. Enter the time period for your query.
4. (Optional) Select the Match check box to enter a match value.
5. Click Add Filter to enter a filter value. You can add multiple values by clicking Add Filter again. Selecting the Exclude check box will filter for any result *except* the value you enter.
6. Click Query.

   The query results appear.

Using Advanced Filters

You can use SQL-based advanced filters to qualify any function that queries the event database, including narrowing queries, refining scheduled reports, or customizing quick filters. The Advanced Filters interface helps you create the appropriate filter syntax by providing a form for entering logics, columns, operators and values according to your filtering requirements.

Note: This section contains a brief overview of the SQL terms used in advanced filters. We recommend a full understanding of SQL, to use advanced filters to their full potential.

The following SQL logical terms join multiple filter statements.

And

Displays the event information if *all* the joined terms are true.

Or

Displays the event information if *any* of the joined terms are true.

The following SQL operators are used by advanced filters to create the basic conditions:

Relational Operators

Include the event information if the column bears the appropriate relation to the value you enter. The following relational operators are available:

- Equal to
- Not Equal to
- Less than
- Greater than
- Less than or equal to
- Greater than or equal to

For example, using *Greater than* would include the event information from your chosen column if its value is greater than the value you set.

Like

Includes the event information if the column contains a pattern you enter, using % to set the pattern you want. For example, L% would return any values beginning with L, %L% would return any values with L included as neither first nor last letter.

Not like

Includes the event information if the column does not contain the pattern you specify.

In set

Includes the event information if the column contains one or more of the values in the comma-separated set you enter.

Not in set

Includes the event information if the column does not contain any of the values in the comma-separated set you enter.

Matches

Includes any event information that matches one or more of the characters that you enter.

Chapter 7: Configure

The Configure tab contains the pages that let you view and maintain application instances and folders, set session information, and configure the CA EEM back-end Server.

Applications (see page 84)

Lets you view or maintain application instance information.

Folders (see page 91)

Lets you list, view, or maintain global folders and application specific folders.

Session (see page 93)

Lets you modify session parameters, synchronize the cache, and test the launch request features.

Embedded IAM Server (see page 98)

Lets you configure the back-end server, view or maintain the password policies, export application, view cached events, and configure SAF location and PassTicket.

Applications

Use the Applications tab to view and maintain application instances.

When an application registers itself to use CA EEM, an application instance is created. That application instance is used to store user details, access policies, calendars, and application-specific user groups and folders.

The application instance object contains installation information and provides configuration information to the CA EEM back-end server and web user interface. These include:

The application-specific user attributes and their associated types

This list controls what user information is displayed, plus what user attributes can be used in access policies.

The resource classes, and their actions and named attributes

This list controls what resource classes can be selected in an access policy, plus what actions and named attributes that resource class contains.

A default cache update time

This provides a default synchronization time that CA EEM clients use to update their cached policies and sessions.

The following applies when attaching an application instance:

When attached to the <Global> namespace

When attached to the <Global> namespace, the <Global> application instance is shown, and all application instances which you have the right to see (read rights on ApplicationInstance). You can unregister applications, and view application information.

When attached to a specific application instance

When attached to a specific application instance, only the <Global> application instance and that application instance are shown. You can view and modify the application.

Application Instances

The Application Instances page lets you to view and maintain application instances.

Note: You can only modify your application instance if you have been granted rights to do so (write rights to ApplicationInstance).

The following buttons appear on the Application Instances page:

Unregister

Unregisters the application instance.

Note: You must unregister an application before you remove CA EEM Server.

Close

Closes the application instance without saving.

The following fields appear in the Application Instance panel:

Name

Specifies the name of the application instance.

Note: Use only alphanumeric characters to prevent display problems.

Label

Specifies the label that is used to attach to this application instance. Set when application instance was registered.

Brand

Specifies the brand set when the application was registered.

Version

Specifies the version set when the application was registered.

Install Date

Specifies the date the application was registered.

Install Identity

Specifies the user who registered this application.

Install Host

Specifies the host name from which this application was registered.

Install Host Address

Specifies the IP address from which this application was registered. Host Address is the IP name or address of the computer on which the application is registered. The IP name or address can be in Internet Packet version 4 (IPv4) or version 6 (IPv6) format.

Install Host Info

Specifies the operating system tag identifying the install host.

Cache Update Time

Specifies the default cache update time (in seconds) that clients attaching to this application instance will use.

Default: 30 seconds

Synchronize Poll Interval

Specifies the interval for the clients to check for notifications at the Server.

The following fields are contained in each User Attributes panel:

User Attributes

Specifies the list of application-specific user attributes this application will save. User attributes are set in the User page, and referenced in the Policy page. Set the user attribute type and give it a name.

Choose from the following types:

text

Specifies a field that contains a text value.

number

Specifies a field that contains a numeric value. You can use the following characters: 0-9, comma (,), or hyphen (-).

password

Specifies a field that contains a masked value as you might see in a password field. Use the type to mask the content of the field from a user.

boolean

Specifies a check box that the user can select.

select

Specifies a drop-down list from which a user can choose a value.

Multi-valued

Specifies that the field can have multiple values. When assigning user attributes, the user is presented with multiple fields to enter values.

The following fields are contained in each Resource Class panel:

Name

Specifies the name of the resource class. Referenced in Viewing/Administering Policies (see page 30) as the Resource Class Name.

Actions

Specifies the actions for this resource class. Referenced in Viewing/Administering Policies (see page 30) as the Action.

Add Action

Lets you add an action.

Note: Use only alphanumeric characters to prevent display problems.

Named attributes

Specifies resource attributes that may be used in policies for this resource class. Referenced in Viewing/Administering Policies (see page 30) under the "named attribute" values in filters.

Add Named Attribute

Lets you add a named attribute.

Note: Use only alphanumeric characters to prevent display problems.

Add Resource Class

Adds a new resource class object.

Note: Use only alphanumeric characters to prevent display problems.

Use Best Match Evaluation Algorithm

If selected, CA EEM filters the matched policies to only include those policies that best match the resource name. The best match algorithm is described as follows:

1. Determine how many characters match (total number of non asterisk characters) in the policy's resource name mask.
2. Determine how many asterisks are in the policy's resource name mask.
3. Only those policies with the most matching characters and the least asterisks are retained.
4. Empty masks ("", "*", and "**") all evaluate to 0 matching characters, 0 asterisks.

Remove ☒

Removes the specified resource class.

The following fields are contained in the Obligation Names panel:

Name

Specifies the name of the obligation. An obligation is application-specific. For example, if a certain event occurs, the application can use results of a query of an obligation policy to send an email to the system administrator, you might specify the name email sysadmin. You must create the obligation here and reference it when you create a policy.

Add Obligation Name

Lets you define a new obligation name.

Note: Use only alphanumeric characters to prevent display problems.

The following appear in the Translations panel:

Add Language

Displays the New Language pane to add a new language.

Add Key

Displays the New Key pane to add a new key that you want to translate. The key can be a name of resource class, action, named attribute, obligation, or user attribute to the application.

View

Displays the View pane for the selected language or key.

Edit

Displays the Edit pane for the selected language or key.

Delete

Deletes the selected language or key.

Add Key

When you add a new resource class, action, named attribute, obligation, or user attribute to the application, it is automatically added as a key after the application is saved. You can also add new keys to the application.

To add a key

1. Click Sort by Key.

   The translations will be sorted by key.

2. Click Add Key.

   A New Key pane appears.

3. Enter the key name and translations for the new key.

   The key and its corresponding translations are added. If the name already exists, a message appears.

4. Click Add Key to add another new key.

   A New Key pane appears.

5. Click Save.

   Saves the changes and a new key is created.

Add Language

When you add a language and its language code to the application, the code is added as a key and the language text is added as the translation to the selected browser language. You can also add translations in other languages for the language name.

To add new language

1. Click Sort by Language.

   The translations will be sorted by language.

2. Click Add Language.

   A new language pane appears.

3. Enter the values for language name and the language code.

   Example: French [fr]

   The language and its corresponding language code are added. If the name already exists, a message appears.

4. Add the translations for the New Language.

   The new language and its corresponding translations are added.

5. Click Add Language to add another language.

   A new language pane appears.

6. Click Save.

   Saves the changes and a new language is added.

Delete Key

When you delete a key from the application, the related application specific data will no longer appear translated in the user interface.

To delete a key

1. Click Sort by Key.

   The translations will be sorted by key.

2. Click Edit for the corresponding key.

   The Key, its associated language, and translations appear.

3. Click Delete Key.

   The key and its corresponding translations are deleted.

   Note: When you delete a key that has a corresponding entry such as, resource class, action, named attribute, obligation, or user attribute in the application, the translations associated with the key are deleted, but the key remains added as translation.

4. Click Save.

   Saves the changes and the key is deleted.

Delete Language

Note: When you delete a default language, only the associated translations are deleted. When you delete a user-defined language, the language and its associated translations are also deleted.

When you delete a language from the application, the application specific data will not appear translated for that particular language.

To delete a language

1. Click Sort by Language.

   The translations will be sorted by language.

2. Click Edit.

   The language and its associated keys appear.

3. Click Delete Language.

   The language and its corresponding keys are deleted.

4. Click Save.

   Saves the changes and the language is deleted.

Folders

Use the Folders tab to view and maintain global folders and application-specific folders. Folders are places to store each object type. For example, global users reside in global folders, and users reside in folders.

By placing objects (users, policies, calendars) within folders, you can then write administrative scoping policies. For instance, you might want to grant a North American administrator write access only to users in a North America folder.

Note: Only folders that you have the right to see as specified on the Policy page are displayed (read rights of Folder and GlobalFolder).

You can select a folder and view, empty, or delete the folder.

The following fields appear in the Folders panel:

New Folder

Displays the new folder dialog. The location of the new folder is a child of the folder next to the corresponding new folder icon.

Folder

Shows or hides the objects contained in the specified folder.

Folders page

Use the Folders page to view and maintain global and application-specific folders.

The following restrictions apply:

- If attached as <Global> (not through an application instance), you can view and administer global folders.
- If attached through an application instance, you can view and administer folders for that application instance.
- You can only modify folders if you have been granted rights to do so (write rights of GlobalFolder and Folder in the Scoping Policies).

The following buttons appear on the Folders page:

Save

Saves the folder.

Delete

Removes the folder and all children.

Empty

Empties the folder by removing all children.

The following fields appear in the Application Folder and Global Folder panels:

Parent Folder

Specifies the name of the parent folder.

Folder Name

Specifies the name of the folder.

Note: Use only alphanumeric characters to prevent display problems.

Session

The Session tab lets you configure current session parameters, synchronize your session's cache with the back-end policies, and test the launch request features.

Configuration (see page 94)

Lets you modify session configuration parameters.

Synchronize Cache (see page 95)

Lets you update your current session's cache.

Synchronize Push (see page 96)

Lets you send notifications to the server and other clients sharing the same application to update the cache.

Test Launch Request (see page 97)

Lets you launch another instance of the web user interface in a new browser window.

Configuration

Use the Configuration page to set your current session parameters. The current session is the current web user interface session.

The following buttons appear on the Session Configuration page:

Save

Saves the session parameters.

Close

Returns to the Configure sub-tab.

The following fields appear in the Session Configuration panel:

Max Search Size

Specifies maximum number of objects returned with each search. Examples of searches include the Users (see page 18) list and the Groups (see page 22) lists.

Default: 2000

Cache Update Time

Specifies the time (in seconds) this session's cache is updated with the CA EEM back-end server. The cache contains all policies and calendars, plus session attributes.

Synchronize Poll Interval

Specifies the interval for the clients to check notifications at the server.

Event Coalesce Time

Specifies the time (in seconds) that this session sends out coalesced events.

Event Drain Time

Specifies the time (in seconds) to wait for events to drain from the client before destroying the events.

Event Delivery Host

Specifies the host to deliver this session's events to. Hostname is the IP name or address of the computer on which the event delivery host is installed and running. The IP name or address can be in Internet Packet version 4 (IPv4) or version 6 (IPv6) format.

Synchronize Cache

Use the Synchronize Cache page to update the current session's cache objects.

Objects updated during a cache synchronization include:

- Calendars and Policies for the currently attached application instance.
- Session attributes (user/usergroup attributes) for the currently attached user, plus any user which you have run a permission check against.

Synchronize Push

You can use the Synchronize Push feature to push the changes in policies and calendar from a client to server and other clients, sharing the same application, before the default cache update time interval.

Note: To notify other client applications you must have a scoping policy with write access to Notify resource.

The following appear in the Synchronize Push panel:

Synchronize TimeOut

Defines the interval in seconds for the client to receive response from the server on the status of other clients.

- Positive value indicates the client receives the status after waiting for the specified period, or immediately after all the clients are updated.
- Zero value indicates the status will be received without any delay.
- Negative value indicates the status will be received after all the clients are updated.

Synchronize

Notifies the change to server and all clients sharing the same application.

Synchronize Remote Clients

Indicates the status of the clients.

Username

Indicates the user name of the client.

Host

Indicates the host name of the client. Hostname is the IP name or address of the computer on which the remote client is installed and running. The IP name or address can be in Internet Packet version 4 (IPv4) or version 6 (IPv6) format.

Status

Indicates the status of the client.

- Updated indicates the client has been updated with the changes.
- Initiated indicates the changes are being updated.
- Not Updated indicates client has not been updated with the changes.

Test Launch Request

Use the Test Launch Request page to launch a new web user interface, in the context you specify.

The following buttons appear in the Test Launch Request panel:

Launch

Exports the current session and launches a new browser window in the specified context.

The following fields appear in the Test Launch Request panel:

Launch Page

Specifies the page to launch into.

Launch Action

Specifies the requested action.

Return Success URI

Specifies the URI the new browser calls when the launched browser page completes successfully.

Return Failure URI

Specifies the URI the new browser calls when the launched browser page fails to complete successfully.

Locale

Specifies the locale to use on the launched page.

Object Name

Specifies the object name to use on the launched page. This is optional, as not all launch actions request an object name.

Resource Names

Specifies a list of resource names to pass with the launch request. These are used when launching access policies.

Add Resource

Lets you add a resource name to the Resource Names list.

CA EEM Server

The CA EEM Server tab lets you manage the following:

Global Users/Global Groups (see page 99)

Lets you configure whether global users are stored internally, or referenced from an external source.

EiamAdmin Password (see page 107)

Lets you set the password for the built-in CA EEM administrator.

Password Policies (see page 108)

Lets you set password policies for internal global users.

Cached Events (see page 108)

Lets you view events cached by the CA EEM Server.

Configure SAF Location (see page 110)

Lets you set the SAF file location to enable Reliable Event Delivery.

Artifact Authentication (see page 111)

Lets you configure the artifact authentication source information.

The following options appear only if you attach to an application instance:

Export Application (see page 114)

Lets you export application objects to an XML file.

PassTicket Configuration (see page 114)

Lets you configure the Mainframe application profile.

Global Users/Global Groups

Use the Global Users/Global Groups page to control whether global users are stored internally, or referenced from an external source. If global users are set from an external source, this page also lets you configure the connection parameters to attach to and reference the external global users.

The following buttons appear on the Global Users/Global Groups page:

Save

Saves the configuration.

Close

Returns to the CA EEM Server tab.

The following fields appear in the Global Users/Global Groups panel:

Store in CA's Management Database (CA-MDB)

Stores the global users and global groups internally. Do not reference an external user source. If selected, you can set Password Policies, and global users and global groups will not be read only.

Reference from an External Directory (see page 100)

Displays global users and groups from an external directory. If selected, global users and global groups are considered read only.

Reference from CA SiteMinder (see page 105)

Displays users and groups from CA SiteMinder data store. If selected, users and groups are considered read only.

Reference from an External Directory

References global users and groups from an external directory. If this is selected, global users and global groups are considered read only.

If Reference from an external directory is selected, the following fields appear:

Type

Specifies the type of external directory. Currently supported types include Custom Mapped Directory, CA Identity Manager, Microsoft Active Directory, Novell eDirectory, Novell eDirectory-CN, and Sun One Directory.

Host

Specifies the host of the external directory. Hostname is the IP name or address of the computer on which the external directory is installed and running. The IP name or address can be in Internet Packet version 4 (IPv4) or version 6 (IPv6) format.

Port

Specifies the port to connect to on the external directory host. This is an LDAP port.

Base DN

Specifies the LDAP DN that is used as the base. Only global users and groups discovered underneath this DN are mapped into CA EEM.

Note: No spaces are allowed in this base DN.

User DN

Specifies the DN to use to attach to the external directory host.

Password and Confirm Password

Specifies the password for the User DN that is used to attach to the external directory host.

Transport Layer Security

Specifies whether to use TLS when making the LDAP connection to the external directory.

Include Unmapped Attribute

Indicates the external attributes that are not mapped.

Note: Unmapped attributes can be used for search and as filters.

Cache Global Users

If selected, CA EEM Server caches in memory the global users. This allows for faster lookups at the cost of scalability.

Note: Global user groups are always cached.

Cache Update Time

Specifies the time (in minutes) to update the cached groups (and optionally users).

Retrieve Exchange Groups as Global User Groups

If selected, then Exchange groups are also used as valid Global User Groups. This lets you write policies against members of distribution lists. Available only for type Microsoft Active Directory.

Status

Specifies the status of the External directory bind and if the External directory data is loaded or not.

- ✅ Means success, and is displayed if the External directory bind is successful and/or data is loaded.
- ⚠ Means warning, and is displayed if the External directory data is still loading.
- ❌ Means error, and is displayed if the External directory bind failed.

Note: To refresh the status, without saving the changes, click Refresh status.

Custom Mapped Directory

You can use Custom Mapped Directory to configure an external directory by providing the required mapping to object classes, user attributes, group attributes, and search filters. With Custom Mapped Directory you can share, retrieve, and reuse the global user and group information, configured in the application.

You can configure CA EEM as the backend Server to use Custom Directory as the Global User Authoritative source.

Note: You must select the source of global users before registering the application instances, as changing the source later affects the applications sharing the same backend server and leads to unmapped user information in applications.

The following appear in the Custom Mapped Directory page:

Label In Use

Specifies the label or name for a configuration. The configuration for the directory is stored using the specified label. It also provides the list of available configurations.

Label ✎

Displays the Custom Directory Mapping panel to view or modify the label.

The following appear in the Custom Directory Mapping page:

Label

Displays the available list of configurations.

New Label 🗋

Displays the create New Label panel.

Save Label

Saves the configuration.

SaveAs

Saves the configuration with different name.

Delete 🗑

Deletes the selected label.

The following fields appear in the Global User Attributes panel:

Global User Class

Defines the user object class in the Custom Directory.

Add Global User Class

Adds User Class to the list.

Delete Global User Class

Deletes the selected User Class.

User Attribute

Specifies the list of Global User Attributes.

Directory Attribute

Defines the mapping for the corresponding directory attribute.

Remove

Removes the attribute.

User Filter

Defines the filter to any search for global users.

Pre User Filter

Defines the filter to any search for a specific user.

Post User Filter

Defines the filter appended to any search for a specific user.

The following fields appear in the Global Group Attributes Panel:

Global Group Class

Specifies the group object class in the Custom Directory.

Add Global Group Class

Adds the group class to list.

Delete Global Group Class

Deletes the selected group class.

Use Group As Container

Specifies that the group is used as a Container.

Unique Member Attribute

Defines the mapping for the corresponding directory attribute.

Use Group As Attribute

Specifies that the group is used as Attribute.

Group Membership Attribute

Defines the mapping for the corresponding directory attribute.

User Membership Attribute

Defines the mapping for the corresponding directory attribute.

Group Filter

Defines the custom filter to any search for global groups.

The following fields appear in the Folder Attributes Panel:

Folder Class

Defines the folder object class in the Custom Directory.

Folder Filter

Defines the custom filter to any single branch search.

Reference from CA SiteMinder

You can use CA EEM to authenticate and authorize the users stored in CA SiteMinder. CA EEM can reference the global user and group's information configured in CA SiteMinder and reuse the global user information and passwords, as read-only.

Note: You must select the source of global users before registering the application instances, as changing the source later affects the applications sharing the same backend server and leads to unmapped user information in applications.

If Reference from CA SiteMinder is selected, the following fields appear:

Host

Defines the name of host system where CA SiteMinder is running. Hostname is the IP name or address of the computer on which the CA SiteMinder is installed and running. The IP name or address can be in Internet Packet version 4 (IPv4) or version 6 (IPv6) format.

Admin Name

Defines the CA SiteMinder super user who has privileges to maintain system and domain objects.

Admin Password and Confirm Password

Defines the password for CA SiteMinder administrator.

Agent Name

Defines the agent's name. This name must match the agent name provided to the Policy Server.

Note: Agent name is not case-sensitive.

Agent Secret and Confirm Secret

Defines the shared secret as defined in the CA SiteMinder user interface.

Note: Agent Secret is case-sensitive.

Cache Global Users

Indicates that CA EEM Server caches the global users in memory. This allows for faster lookups at the cost of scalability.

Note: Global user groups are always cached.

Include Unmapped Attribute

Indicates the external attributes that are not mapped.

Note: These can also be used for search or as filters.

The following fields appear in the User Store Information panel:

Authorization Store Type

Specifies the type of store used by CA SiteMinder for authorization. Currently supported types include CA Identity Manager, Custom Mapped Directory, Microsoft Active Directory, Novell eDirectory, Novell eDirectory-CN, and Sun One Directory.

Authorization Store Name

Specifies the authorization store against which user information is authorized.

Authentication Store Name

Specifies the authentication store against which user information is authenticated.

Search Time Out

Specifies the maximum time for which CA SiteMinder will wait for a response from an external directory when searching users. CA SiteMinder will timeout the connection with an external directory after the specified time.

Default: 60 seconds.

Refresh Store

Retrieves store information (Authorization Store Name and Authentication Store Name) based on the connection parameters.

The following fields appear in the Connection Attributes panel:

Min Connection

Defines the minimum number of connections used by CA SiteMinder.

Default: 1

Max Connection

Defines the maximum number of connections used by CA SiteMinder.

Default: 20

Step Connection

Defines the number of connections to allocate when out of connections.

Limits: 1-20

Connection Time Out

Defines the connection timeout in seconds.

Accounting Port

Defines the accounting port used byCA SiteMinder. Zero indicates there is no accounting port.

Authorization Port

Defines the authorization port used by CA SiteMinder. Zero indicates there is no authorization port.

Authentication Port

Defines the Authentication port used by CA SiteMinder. Zero indicates there is no authentication port.

Status

Specifies the status of the External directory bind and if the External directory data is loaded or not.

- ✓ Means success, and is displayed if the External directory bind is successful and/or data is loaded.
- ⚠ Means warning, and is displayed if the External directory data is still loading.
- ✖ Means error, and is displayed if the External directory bind failed.

Note: To refresh the status, without saving the changes, click Refresh status.

EiamAdmin Password

The EiamAdmin Password page lets you change the password of the built-in administrator.

Note: This page is only available if you are attached as user EiamAdmin.

The following buttons appear on the EiamAdmin Password page:

Save

Saves the new password.

Cancel

Returns to the CA EEM Server tab.

The following fields appear in the EiamAdmin Password panel:

New Password and Confirm Password

Specifies the new EiamAdmin password.

Password Policies

The Password Policies page lets you set the password policies for internal global users.

Note: This page is only available if the global users or global groups are stored internally.

Select the options that you want use in your password policy and then click one of the following buttons:

Save

Saves the updated password policies.

Reset

Resets the display to the currently saved password policies.

Cancel

Returns to the CA EEM Server tab.

Cached Events

Use the Cached Events page to view events that were cached by the CA EEM Server for the attached application instance.

Note: Only events that you have the right to see (view rights in Viewing/Administering Policies (see page 30)) are displayed.

You can view the following events:

- Admin Events
- Runtime Events
- Coalesced Events

Admin Events

Admin Events are generated when CA EEM objects are inserted, removed, or modified (these are referred to as administrative actions).

The following columns appear in the Admin Events panel:

Date

Indicates the date and time the event occurred.

Src

Indicates the application instance label.

Identity

Indicates the identity that performed the administrative action.

Method

Indicates the administrative action performed.

Resource Class

Indicates the resource class of the object.

Resource

Indicates the resource attribute name, and its old and new values.

Runtime Events

Runtime Events are generated when CA EEM methods are invoked, such as authentication and authorization calls. The following columns appear in the Runtime Events panel:

Date

Indicates the date and time event occurred.

Src

Indicates the application instance label.

Identity

Indicates the identity that performed the runtime action.

Method

Indicates the invoked CA EEM method.

Error Code

Indicates the error code that was returned by the CA EEM method.

Resource

Indicates the resource being acted upon (identity, application instance label, or resource name).

Coalesced Events

Coalesced Events are generated for both Admin and Runtime Events. Even if the event policies are set to not submit a specified event, Coalesced Events are still generated on a regular interval (defaults to 300 seconds). Events are coalesced based on unique application instance, method, and status.

The following columns appear in the Coalesced Events panel:

Date

Date and time event occurred.

Src

The application instance label.

Method

The administrative action or CA EEM method invoked.

Status

Success or Failure.

Start Time and End Time

Defines the coalesce interval.

Count

Specifies the number of events coalesced.

Configure SAF Location

The Configure Store-and-Forward (SAF) Location page lets you enable Reliable Event Delivery to ensure all the events generated using the CA EEM web interface reach the CA EEM Server.

For more information on Reliable Event Delivery, see the *Programming Guide*.

The following fields appear on the SAF Configuration page:

SAF File Location

Defines the location to store and forward events.

Example: C:\\<*Folder Name*>

The following buttons appear on the SAF Configuration page:

Save

Saves the configuration.

Close

Returns to the CA EEM Server tab.

Artifact Authentication

You can use the Artifact Authentication to enable single sign-on from any web access management application that issues SAML artifacts to any CA EEM embedded application.

Note: The identity provider (source site) must be configured for Browser Artifact profile, to generate SAML artifacts.

The following buttons appear on the Artifact Authentication page:

Save

Saves the configuration.

Close

Closes the page.

The following options appear:

- Authenticate against internally generated artifacts only
- Authenticate against internally generated artifacts and external SAML server

The following fields appear on selecting the Authenticate against internally generated artifacts and external SAML server:

Service Provider ID

Defines the unique name that identifies the service provider (relying party). Some implementations of the asserting party use this ID to validate the artifact with the service provider, for which the ID is generated.

The following fields appear in the Key Store Information panel:

File Location

Defines the location of the key store file.

Store Type

Specifies the type of key store. Currently supported types include JKS and PKCS12.

Signing Key Alias

Defines the alias in the key store that stores the private key. It is used to sign the SAML Request if Sign Request is enabled.

Store Password and Confirm Password

Defines the key store password.

The following fields appear in the Trust Key Store Information panel:

File Location

Defines the location of the trust key store file.

Store Type

Specifies the type of the trust key store. Currently supported types include JKS and PKCS12.

Store Password and Confirm Password

Defines the trust key store password.

The following appear in the Artifact Source Information panel:

Add Artifact Source Information

Displays the add source information panel.

Delete

Deletes the source information.

Host

Defines the host name of the identity provider (source site). Hostname is the IP name or address of the computer on which the identity provider is running. The IP name or address can be in Internet Packet version 4 (IPv4) or version 6 (IPv6) format.

Sign Request

Specifies if the request sent to the asserting party must be signed.

Assertion Attribute

Defines the attribute in the assertion that will be used to set the identity of the session created during the AuthenticateWithArtifact API call. The asserting party can specify the attributes that can be included in the assertions, as part of their configuration.

Source ID

Defines the source ID of the asserting party.

Responder URL

Defines the URL to which the SAML request is sent to retrieve the assertion corresponding to the artifact.

Configure Artifact Authentication

You can configure CA EEM for artifact authentication.

To configure artifact authentication

Note: Ensure you log into CA EEM with administrator privileges.

1. Select Authenticate against internally generated artifacts and external SAML server.
2. Enter the value for Service Provider ID, Key Store File Location, and Signing Key Alias.
3. Select the Storage Type:
   - JKS—keystore implementation provided by the SUN provider.
   - PKCS#12—transfer syntax for personal identity information.
4. Enter the values for Trust Key Store File Location, Store and Confirm Password

   Note: If you modify the Key Store or Trust Key Store file information, you must restart iGateway for the changes to apply.
5. Select the Storage Type.
6. Click Save.

   Saves the changes and the Artifact Authentication is configured.

Add Artifact Source Information

You can use the Add Artifact Source Information to provide information about the source from where the artifact is generated.

To add artifact source information

1. Click Add Artifact Source Information.

   The Artifact Source Information panel appears.
2. Enter the values for Host, Assertion Attribute, Source ID, and Responder URL.
3. Click Save.

   Saves the changes and Artifact Source Information is added.

Export Application

The Export Application page lets you export the application objects to an XML file. You can use the export feature to export an application and save a backup copy, or to migrate your application from a test to a production environment.

To export an application to XML

1. Select the objects you want to export to the XML file.
2. Click Export.

   A dialog appears with options to open or save the XML file.

PassTicket Configuration

The PassTicket Configuration page lets you configure the mainframe application profile to define the Application Profile ID and the Secure Sign-on (SSKEY) fields.

For more information on PassTicket Configuration, see the *Programming Guide.*

The following fields appear in the Application Host Information pane, if you select Enable PassTicket Generation:

Application Profile ID

Defines the 1 - 26 character profile name of the corresponding application. The record ID is determined by four distinct combinations of an application name, group name, and user ID. The combinations are as follows:

- application.group.userid
- application.userid
- application.group
- application

SSKey

Defines the 16-character hexadecimal representation of the eight-byte encryption key for the mainframe application.

The following buttons appear on the PassTicket Configuration page:

Save

Saves the configuration.

Close

Returns to the CA EEM Server tab.

Index