CA GREEN BOOKS

CA IT Client Manager / CA Unicenter Desktop and Server Management

Object Level Security Best Practices

Transforming IT Management

LEGAL NOTICE

This publication is based on current information and resource allocations as of its date of publication and is subject to change or withdrawal by CA at any time without notice. The information in this publication could include typographical errors or technical inaccuracies. CA may make modifications to any CA product, software program, method or procedure described in this publication at any time without notice.

Any reference in this publication to non-CA products and non-CA websites are provided for convenience only and shall not serve as CA's endorsement of such products or websites. Your use of such products, websites, and any information regarding such products or any materials provided with such products or at such websites shall be at your own risk.

Notwithstanding anything in this publication to the contrary, this publication shall not (i) constitute product documentation or specifications under any existing or future written license agreement or services agreement relating to any CA software product, or be subject to any warranty set forth in any such written agreement; (ii) serve to affect the rights and/or obligations of CA or its licensees under any existing or future written license agreement or services agreement relating to any CA software product; or (iii) serve to amend any product documentation or specifications for any CA software product. The development, release and timing of any features or functionality described in this publication remain at CA's sole discretion.

The information in this publication is based upon CA's experiences with the referenced software products in a variety of development and customer environments. Past performance of the software products in such development and customer environments is not indicative of the future performance of such software products in identical, similar or different environments. CA does not warrant that the software products will operate as specifically set forth in this publication. CA will support only the referenced products in accordance with (i) the documentation and specifications provided with the referenced product, and (ii) CA's then-current maintenance and support policy for the referenced product.

Certain information in this publication may outline CA's general product direction. All information in this publication is for your informational purposes only and may not be incorporated into any contract. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document "AS IS" without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, lost investment, business interruption, goodwill or lost data, even if CA is expressly advised of the possibility of such damages.

COPYRIGHT LICENSE AND NOTICE:

This publication may contain sample application programming code and/or language which illustrate programming techniques on various operating systems. Notwithstanding anything to the contrary contained in this publication, such sample code does not constitute licensed products or software under any CA license or services agreement. You may copy, modify and use this sample code for the purposes of performing the installation methods and routines described in this document. These samples have not been tested. CA does not make, and you may not rely on, any promise, express or implied, of reliability, serviceability or function of the sample code.

TITLE AND PUBLICATION DATE:

Object Level Security Best Practices Green Paper
Publication Date: August 6, 2009

ACKNOWLEDGEMENTS

Principal Authors

Reinhold Jaekle

The principal authors and CA would like to thank the following contributors:

CA Services

Development

Marketing

QA

Support

SWAT

Technical Sales

Technical Information

Third-Party Acknowledgements

Microsoft product shots reprinted with permission from Microsoft Corporation. Microsoft and Windows are registered trademarks of Microsoft Corporation in the United States and other countries.

CA PRODUCT REFERENCES

This document references the following CA products:

- CA IT Client Manager (CA ITCM), formerly CA Desktop and Server Management (DSM)

FEEDBACK

Please email us at greenbooks@ca.com to share your feedback on this CA Green Publication. Please include the title of this Green Publication in the subject of your email response. For technical assistance with a CA product, please contact CA Technical Support at http://ca.com/support. For assistance with support specific to Japanese operating systems, please contact CA at http://www.casupport.jp.

Contents

PREFACE

CA IT Client Manager (CA ITCM) is the new comprehensive solution that replaces the stand-alone products within the CA Client Management Solution. CA IT Client Manager combines the following products into one fully functional solution:

- CA Asset Management (formerly Unicenter Asset Management)
- CA Asset Intelligence (formerly Unicenter Asset Intelligence)
- CA Software Delivery (formerly Unicenter Software Delivery)
- CA Remote Control (formerly Unicenter Remote Control)
- CA Patch Manager (formerly Unicenter Patch Management)
- CA Desktop Migration Manager (formerly Unicenter Desktop DNA)

This document focuses on various components of the new CA IT Client Manager solution, and therefore has used the old product names when addressing these functional areas.

Chapter 1: Introduction

This document contains information that gives you a deeper look and a better understanding of the Object Level Security feature. The document is a supplement to the product documentation provided with the components of the CA ITCM solution. The guidelines and best practices are provided to assist you with setting up a CA ITCM environment that fits the security needs of your enterprise.

Document Scope

The security features in CA ITCM cover the following subject areas:

Authentication

Provides confidence that the requesting object is what it says it is.

Authorization

Provides the configuration and validation of access rights and privileges for performing operations on secured objects.

This document focuses on Authorization *only*.

Audience

This document is intended for administrators working with CA ITCM. It provides useful information that enables an administrator to set up and customize the security settings in an existing CA ITCM installation on the Domain Tier and Enterprise Tier.

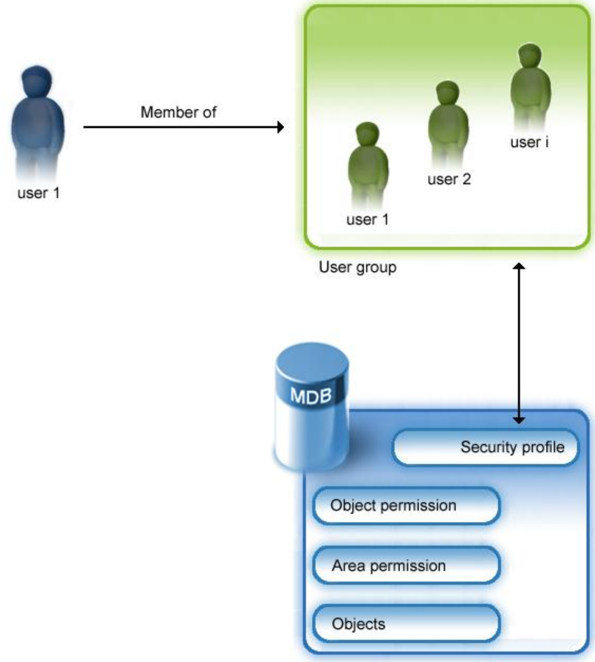
Chapter 2: Object Level Security

The CA IT Client Manager (CA ITCM) management database provides class and object-level security (OLS). The permissions assigned in the database are associated with a security profile, which is represented by an object Uniform Resource Identifier (URI). Certificate URIs can be associated with security profiles and therefore can be used to regulate access to the CA ITCM management database.

Authorization

Authorization controls the rights and privileges for an object associated with an authenticated entity, typically, a logged-in user. An authenticated entity is managed by security profiles. This means that a user or a user group is represented by a security profile and all permissions are managed in connection with the security profile.

The CA ITCM security subsystem manages the authorization by providing a robust and generic security option for the entire CA ITCM system. It is responsible for controlling the rights and privileges for an object associated with an authenticated entity named security profile. The following illustration shows a standard scenario where a user is a member of a user group.



The terms *user* and *user group* refer to a directory user account and a directory user group definition. As illustrated earlier, the user group is represented by a security profile definition which is stored in the MDB.

In addition, the MDB stores the permissions as assigned to security profiles. If a user launches the DSM Explorer or runs a DSM command line utility, then each user request will be processed based on the permissions as defined for the security profiles that the user is a member of.

For example, you can create security profiles to determine which operating system-dependent groups and users can access the CA ITCM system. You can also establish class permissions, group and object permissions, and restrict the access of users or user groups to selected folders or objects.

Security Profiles

A *security profile* is an operating system user account or group either in the domain manager (local profiles) or in its network domain (domain profile).

The security subsystem in CA ITCM supports multiple security profiles. A security profile is either built-in (that is, created during installation) or user-defined.

A user-defined security profile represents either a single user or a user group.

The most important security profiles created during installation include:

- Owner (virtual account, represents the owner of an object)
- Everyone (default virtual account for all users)

In addition to the security profile, a set of security classes is associated with a profile. The security classes are the same across all security profiles, but each security profile has different permissions to the classes. A security class allows setting the permissions that will be assigned to an instance of such a class as soon it is created.

You can also create security profiles for users in the trusted domains. Every user is required to have a valid security profile to log in to the system. If new users are added to a managed group, they automatically inherit the access rights given to the group and can log in to the system instantly.

Single user, multiple profiles

A user can have multiple profiles. However, each profile can be mapped to only one user or group. For example, if a user is a member of a group, then that user can have two profiles—one mapped to the user account and the other mapped to the group. In this case, the user will have the [mathematical] union of permissions in both profiles.

If a user is a member of more than one security profile, then the effective permission for that user is a [mathematical] union of the individual permissions defined for each security profile (like applying [mathematical] OR to all permissions).

Remove or deny access

If you want to deny access for a user of an individual security profile, you must remove that user from the security profile. In case a user is member of more than one security profile or group, then it is required to remove the user from all security profiles.

CA ITCM provides predefined security profiles and lets you create as many profiles as you want using the Security Profiles dialog.

We recommend that at least one of these profiles has Full Control as access rights to the system.

Permissions

Authorization covers the following types of permissions:

Class permissions

Permissions that act as the default permission assigned to every object of the class.

Object permissions

Permissions that are assigned individually for a single object.

Area permissions

Permissions that are used to define which objects are visible in an area.

A Permission definition is represented by an access control entry (ACE), which represents the following permissions:

ACE	Description	Remarks
V	View	Allows you to show objects
R	Read	Allows you to read sub-objects of an object; for example, members of a group
C	Create	Allows you to create objects
W	Write	Allows you to change an object
X	Execute	Allows you to execute objects; depends on the type of the object
D	Delete	Allows you to delete objects
P	Permission	Allows you to change the permission itself
O	Ownership	Allows you to take ownership of an object

The security subsystem manages all types of permissions and uses a cumulative approach to reach the effective permissions.

Note: If you have enabled area permissions, then both object and area permissions are selected to get access to objects. In this case, users need object permissions and area permissions to manage objects. If area support is disabled, then only object permissions are selected.

Chapter 3: Use Cases

The following sections describe the various use cases such as CA ITCM Administration use case, Software Delivery use case, and so on.

The general use cases are as follows:

Manage collect tasks

Manage AM collect jobs.

Manage collection modules

Manage inventory modules for inventory detection and inventory templates.

Manage configuration policies

Create, modify, or delete computer policies.

Manage configuration view

Configuration views are not subject to security.

Manage configuration jobs

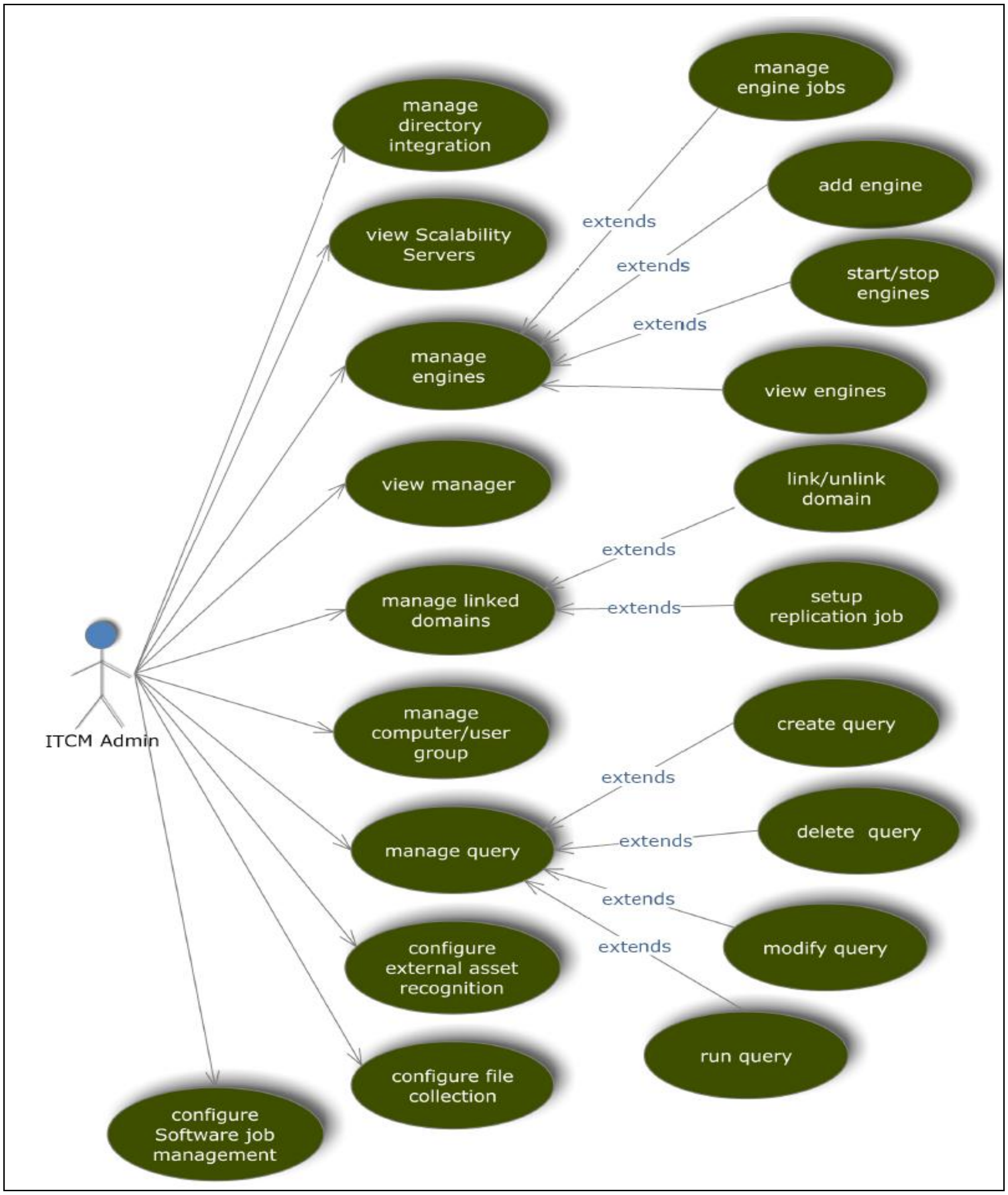
Create or delete configuration jobs for computers asset groups.

Manage configuration reports

View or request configuration reports for computers.

CA ITCM Administration Use Cases

The following illustration shows the major CA ITCM administration use cases. This illustration covers all activities that are related to the infrastructure and configuration of CA ITCM as queries and groups.



Actors

The actor in the CA ITCM administration use case, and his or her scope is as given below:

CA ITCM Administrator

The owner of CA ITCM responsible for setting up its environment.

Tasks on Directory Integration

The following table gives details of tasks, security classes the tasks belong to, and the corresponding permission required on these classes.

Task	Security Class	Permissions
General GUI access	Domain Control Panel Access Configured Directory	VR
Add directory	Configured Directory	CW
Delete directory	Configured Directory	D
Change properties	Configured Directory	W
Configure directory sync job	Engine Engine Task	VRW

Permissions for Directory Integration

The following permissions are available for directory integrations:

Create (C)

Adds a configured directory.

View (V) and Read (R)

Lets you navigate to and access Directory Integration in the Control Panel.

Delete (D)

Lets you delete a configured directory.

Execute (X)

This permission is not used in this scenario.

Write (W)

Lets you add or change the properties of a configured directory, and configure the engine job.

Permission (P)

This permission is not used in this scenario.

Tasks on Engine

The following tasks are available on the engine:

Task	Security Class	Permissions
General GUI access	Domain Control Panel Access Engine	VR VR VR
Create a new engine instance	Engine	C
Start or stop engine	Engine Administrator user rights on the machine where the engine runs	X
Create engine task	Engine Engine Task	W C
Link or unlink existing task to the engine	Engine Engine Task	W VR

Task	Security Class	Permissions
Editing engine task properties or status	Engine Task	VRW
Set as next task to be executed	Engine Engine Task	X VR
Changing the order of engine task	Engine Engine Task	W VR
Link or unlink a domain	Domain Domain Group	VRW VR
Configure replication job	Engine Engine Task	W VRW

Permissions for Engine

The following permissions are available on the engine:

Create (C)

Lets you create an engine instance or engine task.

View (V) and Read (R)

Lets you navigate to and access the engine and engine tasks in the Control Panel.

Delete (D)

Lets you delete an engine instance.

Execute (X)

Lets you start or stop engine instance, and set task ordering.

Write (W)

Lets you create, link or unlink, and edit the engine task.

Permission (P)

This permission is not used in this scenario.

Tasks on Replication

The following table gives details of tasks on replication, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access View domains	Domain Domain Group Control Panel Access	VR
Link or unlink a domain	Domain	W
Configure replication job	Engine Engine Task	VRW

Permissions for Replication

The following permissions are available on replication:

Create (C)

This permission is not used.

View (V) and Read (R)

View permission is required to view the properties of a domain.

Read permission is required to list the members of a domain group.

Both View and Read permissions are required to navigate to access domains in the Control Panel.

Delete (D)

This permission is not used in this scenario.

Execute (X)

This permission is not used in this scenario.

Write (W)

Lets you link or unlink a domain and configure a replication job.

Permission (P)

This permission is not used in this scenario.

Tasks on Groups

The following table gives details of tasks on groups, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
Create a group	Asset Group Server Group Domain Group	RVCW
Delete a group	Asset Group Server Group Domain Group	RVDW

Task	Security Class	Permissions
Search computer	Computer	RV
Search user account	User	RV
Search profile	Computer User	RV
Power up computer	Computer Computer User Asset Group	RX
Add computer	Asset Group	RP
Set permissions	Asset Group	RVP
Set software rights	Domain	VR
	Asset Group	VRW
	Software Definition	VR

Permissions for Groups

The following permissions are available on groups:

Create (C)

Lets you create an Asset, Server, or Domain Group. This permission is required on the class.

View (V)

Lets you search for a Computer, User Account or User Profile.

Read (R)

Lets you power up a group of Computers or User Profiles. This permission is required on the group.

Delete (D)

Lets you delete an Asset, Server, or Domain Group. This permission is required on the group.

Execute (X)

Lets you power up a Computer or User Profile.

Write (W)

Lets you create or delete a group, or add a computer under the parent group. This permission is required on the parent group.

Permission (P)

Lets you change the permissions on the group. This permission is required on the group.

Tasks on Queries

The following table gives details of tasks on queries, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain Common Query	VR
Create query	Common Query	VC
Delete query	Domain	VRD

Task	Security Class	Permissions
Create new query folder	Common Query	V
Import definition	Common Query	C
Run query	Common Query	VRX
Submit to engine (first available)	Common Query	VR
Submit to engine (specific engine)	Common Query Engine	VR VR
Export definition	Common Query	VR
Copy query	Common Query	VRC
Rename query	Common Query	VRW
Set permissions	Common Query Security Profile	VRP V
Modify properties	Common Query	VRWX

Permissions on Queries

The following permissions are available on queries:

Create (C)

Lets you create, copy, or import a query definition. This permission is required on the class.

View (V)

Lets you view queries, create, rename, or delete query folders, and access query wizards.

Read (R)

Lets you view the pre-defined queries and query properties.

Delete (D)

Lets you delete a query.

Execute (X)

Lets you run a query and modify the properties of the query.

Write (W)

Lets you modify the properties of the query and to rename the query.

Permission (P)

Lets you change the permission on the query.

Tasks on External Asset Definition

The following table gives details of tasks on External Asset Definition, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain Control Panel Access	VR V
Create external asset definition	External Asset	C
Delete external asset definition	External Asset	D
Modify properties	External Asset	VC

Permissions on External Asset Definition

The following permissions are available on external asset definition:

Create (C)

Lets you create external asset definitions or modify the external asset definition properties. This permission is required on the class.

View (V)

Lets you view the external asset definition and properties.

Read (R)

This permission is not used in this scenario.

Delete (D)

Lets you delete an external asset definition.

Execute (X)

This permission is not used in this scenario.

Write (W)

This permission is not used in this scenario.

Permission (P)

This permission is not used in this scenario.

Tasks on File Collection

The following table gives details of tasks, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain Control Panel Access	VR V
List file collection definition	Control Panel Access	V
Create file collection definition	File Permissions	Administrator/root

Tasks on Scalability Server

The following table gives details of tasks on Scalability Server, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain Control Panel Access Server Server Group	VR
View Scalability Servers	Control Panel Access Server Server Group	VR

Permissions for Scalability Server

The following permissions are available on the Scalability Server:

Create (C)

This permission is not used in this scenario.

View (V) and Read (R)

View permission is required to view the properties of a Server.

Read permission is required to list the members of a Server Group.

View and Read permissions are required to navigate to and access Scalability Servers in the Control Panel.

Delete (D)

This permission is not used in this scenario.

Execute (X)

This permission is not used in this scenario.

Write (W)

This permission is not used in this scenario.

Permission (P)

This permission is not used in this scenario.

Tasks on Managers

The following table gives details of tasks on Managers, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
View Manager	Control Panel Access	VR

Permissions for Managers

The following permissions are available on Managers:

Create (C)

This permission is not used in this scenario.

View (V) and Read (R)

View permission is required to view the properties of a Manager.

View and Read permissions are required to navigate to and access Manager in the Control Panel.

Delete (D)

This permission is not used in this scenario.

Execute (X)

This permission is not used in this scenario.

Write (W)

This permission is not used in this scenario.

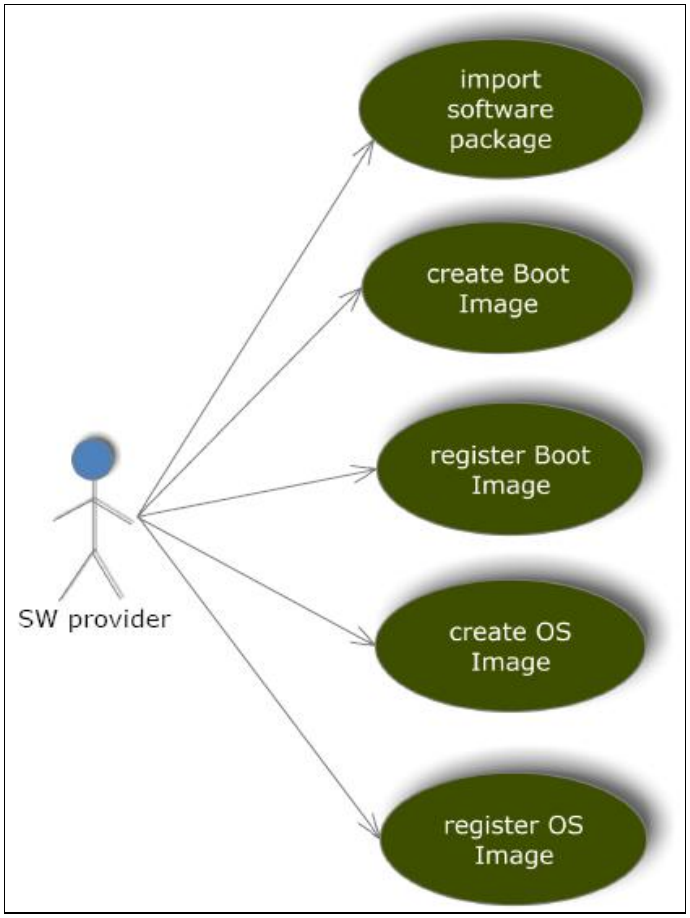
Permission (P)

This permission is not used in this scenario.

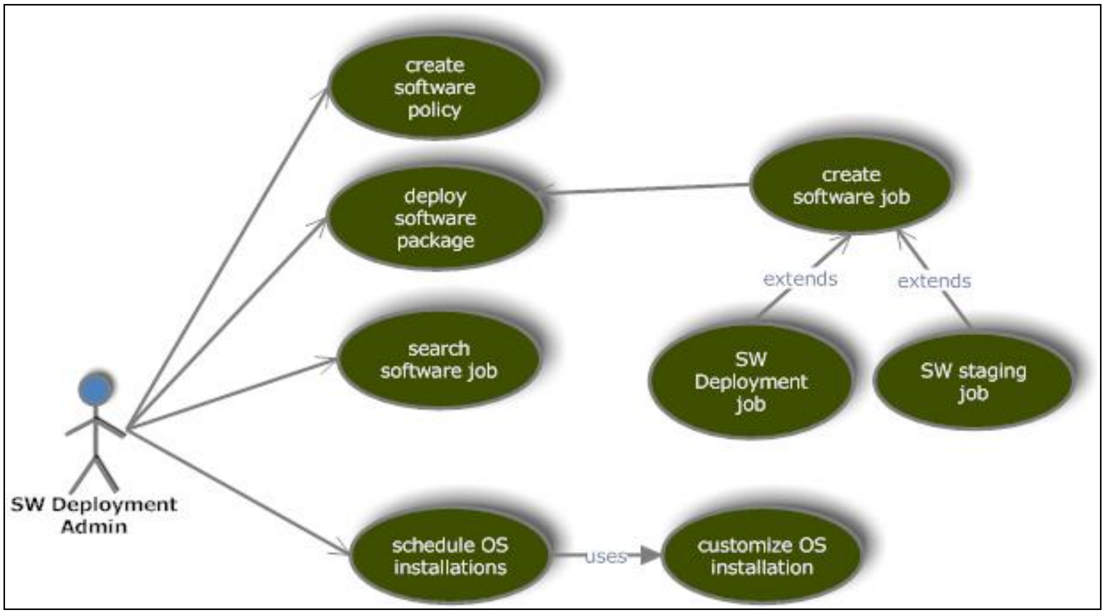
Software Delivery Use Cases

The following illustration shows the use cases for providing the following software:

- A software package that can be distributed via DSM Software Delivery Catalog
- An operating system (OS) image
- A boot image



The following illustration shows the use cases for distributing software:



Actors

The actors in the software delivery use case, and their scope is as given below:

Software provider

> Provide software applications and/or image to make it available for publishing or deployment.

Software deployment administrator

> Responsible for deploying software applications and scheduling operating system installations.

Tasks on Software Jobs

The following table gives details of tasks, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
View software jobs under Jobs – software jobs folder	Software Jobs Software Job Container	V VR
Modify software jobs under Jobs	Software Jobs	VW

Task	Security Class	Permissions
– software jobs folder	Software Job Container	VRW
View software job under a computer folder	Computer Asset Group	R VR
Remove software job under a computer folder	Computer Asset Group	RW VR

Tasks on Packages and Procedures

The following table gives details of tasks on packages and procedures, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain Software Group	VR V
View Software Package	Software Group Software Package	VR V
View Software Package and Procedure	Software Group Software Package Procedure	VR VR V
Create Software Package	Software Group Software Package	VRW C
Modify Package	Software Group Software Package	VR VW
Create Procedure (Unseal the package, delete procedure, and then seal the package).	Procedure Software Group Software Package File permissions	C VR VRW Administrator/root
Delete Procedure (Unseal the package, delete procedure, and then seal the package).	Procedure Software Group Software Package File permissions	VD VR VRW Administrator/root
Modify Procedure (Unseal the package, modify procedure, and then seal the package).	Procedure Software Group Software Package	VW VR VRW

Task	Security Class	Permissions
	File permissions	Administrator/root

OS Installation Management Tasks on Computers

The following table gives details of tasks on operating system (OS) installation management, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain Asset Group	VR VR
Show OS installations	Computer	VR
Show OS installation parameters	Computer OS Installation Image	VR V
Edit or reset OS installation parameter	Computer OS Installation Image	VRW V
Enable computer for OS installation management	Computer	VRW
Paste or drop OS image to install	Computer OS Installation Image	VRW V
Activate, reinstall, renew, stop, or abort OS installation	Computer	VRX
Manage (unnamed computer)	Computer OS Installation Image	VRC V
Manage (named computer)	Computer OS Installation Image	VRW V
Move To Boot Server	Computer	VRW
Delete from OS installation management	Computer	VRD

Task	Security Class	Permissions
Delete (failed, stopped, or planned)	Computer	VRW
OS installation wizard (assign OS image)	Computer OS Installation Image	VRW V
OS installation wizard (set up OS installation)	Computer OS Installation Image	VRX V

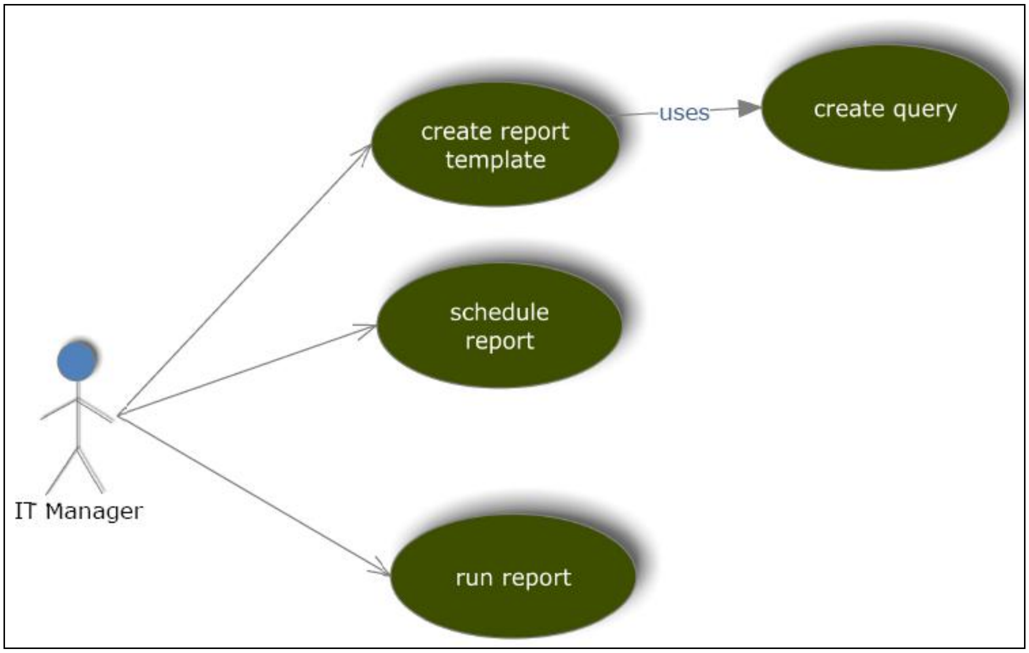
Tasks on Boot and OS Images

The following table gives details of tasks on Boot and OS images, security class the tasks belong to, and the corresponding permission required on these classes.

Tasks	Security Class	Permissions
General GUI access	Domain	VR
Image Prepare System access to create, show, customize and delete local Boot/OS Images	None	Local admin rights
Register Boot/OS Image	None OS Installation Image	Local admin rights C
Show (registered) Boot/OS Images	OS Installation Image	V
Edit Default Value (of an OS Installation Parameter)	OS Installation Image	VW
Delete (registered) Boot/OS Image	OS Installation Image	VD

Reporter Use Cases

Typically, an IT Manager or administrator is interested in reports that provide information about the state of the existing IT infrastructure. These reports can be used as a baseline for making decisions about costs, investments, and so on. The following illustration shows the use cases for reporting.



Actors

The actor for the reporter use case, and his or her scope is as given below:

IT Manager

Is a person who needs statistical data or reports, which can be used for the following purposes:

- Deciding investments
- Auditing
- Provisioning
- Configuration and change-planning (for example, migration projects)

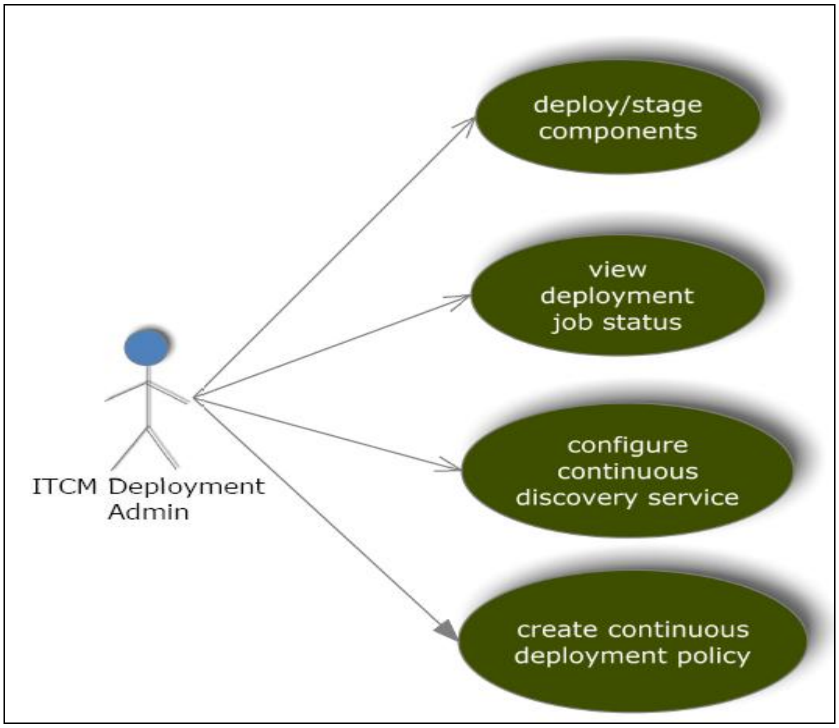
Tasks on Report Templates

The following table gives details of tasks, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Create a report template (New one or import existing report definition)	Report Template	CW
Run Report	Report Template	VRX
Delete Report	Report Template	RWD
Create Schedule Report Template	Report Scheduling Engine Report Template	CRW RW CRW

CA ITCM Deployment Use Cases

The following illustration shows the use cases for deploying the infrastructure for CA ITCM. The deployment activities frequently include rolling out CA ITCM agents to new systems.


deploy/stage components
view deployment job status
configure continuous discovery service
create continuous deployment policy
ITCM Deployment Admin

Actors

The actor for the CA ITCM deployment use cases, and his or her scope is as given below:

CA ITCM deployment administrator

Responsible for deploying the CA ITCM infrastructure.

Tasks on Deployment Job

The following table gives details of tasks, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Deploy Software	Control Panel Access Deployment Job	R C

Permissions for Deployment Job

The following permissions are available on the deployment job:

Create (C)

Lets you create a deployment job with the deployment wizard or a Continuous Discovery Policy using the Continuous Discovery Policy wizard.

View (V)

This permission is not used.

Read (R)

Lets you see the Deployment Jobs node, and Continuous Discovery Policy node.

Delete (D)

Lets you delete a deployment job, or Continuous Discovery Policy.

Execute (X)

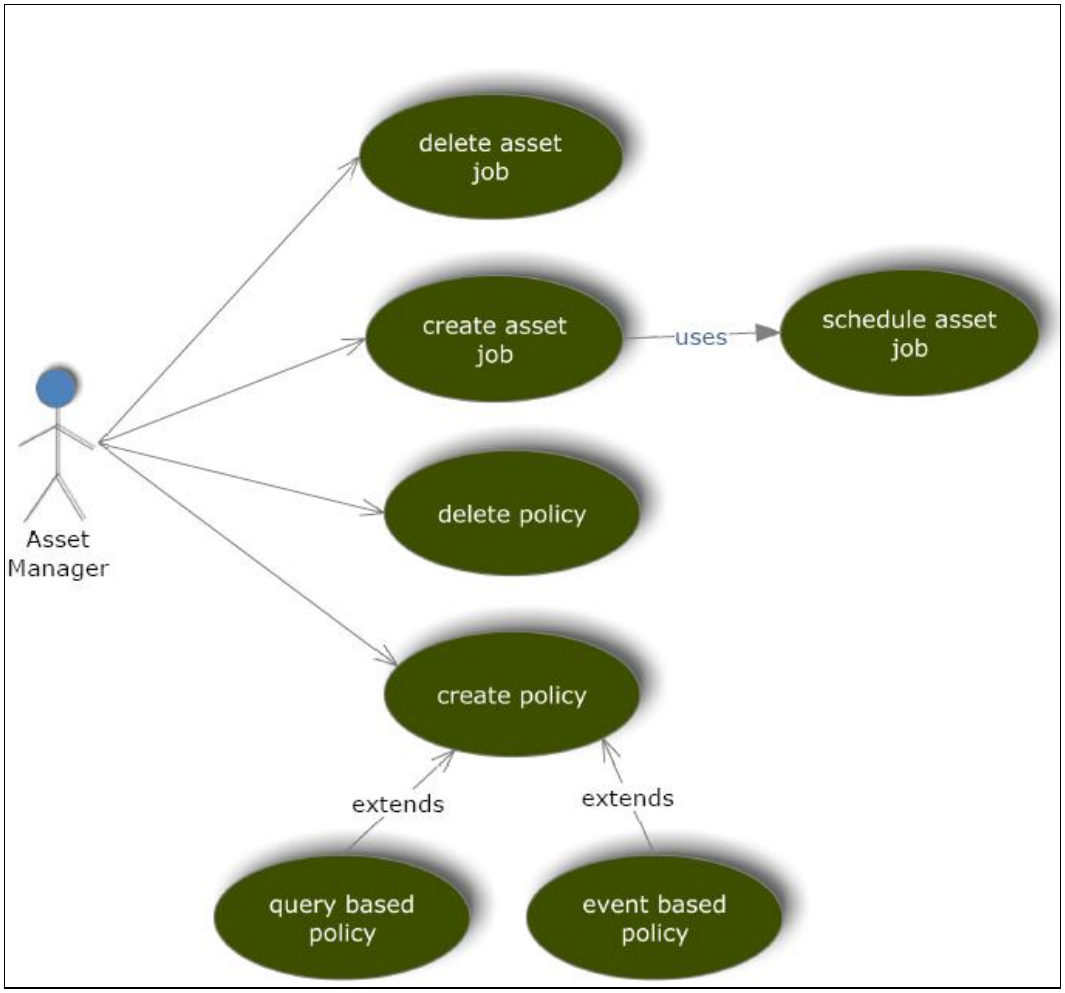
This permission is not used.

Write (W)

Lets you enable, disable, or modify a Continuous Discovery Policy.

Asset Management Use Cases

The following illustration shows the use cases for managing assets.



Actors

The actor for the asset management use case, and his or her scope is as given below:

Asset Manager

Responsible for managing assets.

Tasks on Asset Jobs

The following table gives details of tasks on asset jobs, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Create asset job folder	Asset Job	V
Delete asset job folder	Asset Job	V
Rename asset job folder	Asset Job	V
Create asset job	Asset Job	C
Delete asset job	Asset Job	VRD
Set scheduling for an asset job	Asset Job	VRW
Reinitialize checksum for an asset Job	Asset Job	VR
Rename asset job	Asset Job	VRW
Set permission on asset job	Asset Job Security Profile	VRP V
Modify properties of an asset job	Asset Job	VRWX

Permissions for Asset Jobs

The following permissions are available on asset jobs:

Create (C)

Lets you create an asset job.

View (V)

Lets you create, rename, or delete Asset Job folders.

Read (R)

Lets you view the asset job properties and reinitialize checksum for an asset job.

Delete (D)

Lets you delete an asset job.

Execute (X)

Lets you modify the asset job properties.

Write (W)

Lets you rename or set the scheduling and modify the asset job properties.

Permission (P)

Lets you change the permission for the asset job.

Tasks on Query-Based Policies

The following table gives details of tasks on query-based policies, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Create policy folder	Policy-Query Based	V
Delete policy folder	Policy-Query Based	V
Rename policy folder	Policy-Query Based	V
Create policy	Policy-Query Based Common Query	VC VR
Delete policy	Policy-Query Based	VRD
Rename policy	Policy-Query Based	VRW
Set permissions	Policy-Query Based	VRP

Task	Security Class	Permissions
	Security Profile	V
Modify properties	Policy-Query Based	VRW
Disable policy	Policy-Query Based	VRW
Evaluate now a policy	Policy-Query Based	VR
View query	Policy-Query Based	VR
New action on policy	Policy-Query Based	VRW

Permissions for Query-Based Policies

The following permissions are available on query-based policies:

Create (C)

Lets you create a query-based policy.

View (V)

Lets you create, rename, or delete query-based policy folders.

Read (R)

Lets you view policy properties, and query and evaluate the policy.

Delete (D)

Lets you delete the policy.

Execute (X)

This permission is not used.

Write (W)

Lets you rename, disable, and modify the policy properties.

Permission (P)

Lets you change the permission for the policy.

Tasks on Event-Based Policies

The following table gives details of tasks on event-based policies, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
Create policy	Policy-Event Based	VC
Delete policy	Policy-Event Based	VRD
Rename policy	Policy-Event Based	VRW
Set permissions	Policy-Query Based Security Profile	VRP V
Modify properties	Policy-Query Based	VRW
Disable policy	Policy-Query Based	VRW
New action on policy	Policy-Query Based	VRW

Permissions for Event-Based Policies

The following permissions are available on event-based policies:

Create (C)

Lets you create an event-based policy.

View (V)

Lets you create, rename, or delete event-based policy folders.

Read (R)

Lets you view the policy properties.

Delete (D)

Lets you delete the policy.

Execute (X)

This permission is not used.

Write (W)

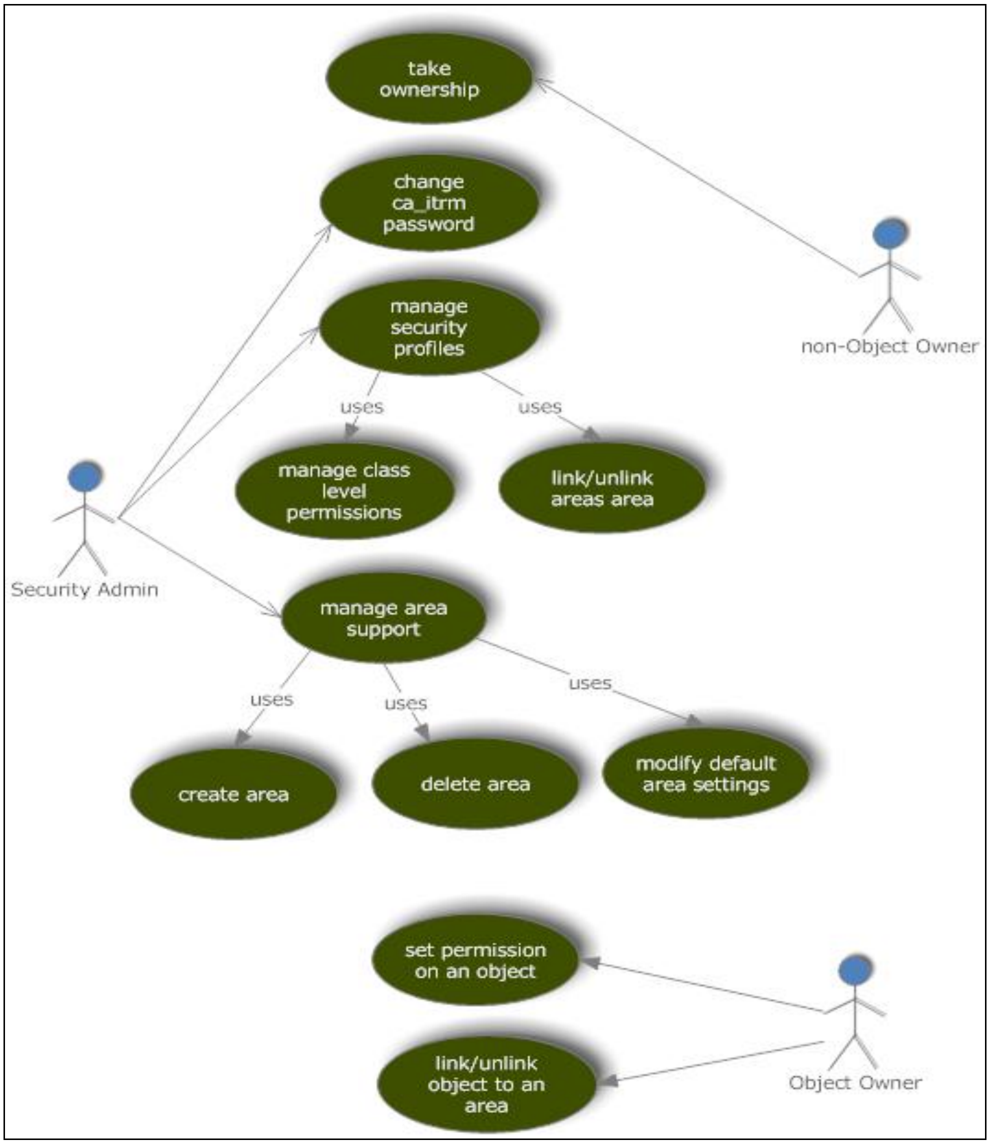
Lets you rename, disable, and modify the policy properties.

Permission (P)

Lets you change the permission for the policy.

Security Administration Use Cases

The following illustration shows the use cases to set up and customize the security settings in an existing CA ITCM environment.



Actors

The actors for the security administration use cases, and their scope is as given below:

Security administrator

Responsible for managing the security environment of CA ITCM.

Object owner

Any user who can access CA ITCM through DSM Explorer, Web Admin Console, or Command Line Interface.

The Object Owner has an object created *directly* or *indirectly*.

Note: The term *directly* refers to an object created manually. The term *indirectly* refers to an object that was created indirectly, for example, at the time of deployment.

Non-Object owner

Any user who can access CA ITCM through the DSM Explorer, Web Admin Console, or Command Line Interface.

The user is able to see an object that was not created either directly or indirectly.

Tasks on Security Profiles

The following table gives details of tasks on security profiles, security class the tasks belong to, and the corresponding permission required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Show security profiles	Security Profile	V
Delete security profile	Security Profile	VD
Add security profile	Security Profile	C
Re-map security profile	Security Profile	VW
Turn area support on or off	Security Profile	VW
Link security profile to security area	Security Profile Security Area	VW V

Tasks on Security Areas

The following table gives details of tasks on security areas, security class the tasks belong to, and the corresponding permission required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Show security areas	Security Area	V
Delete security area	Security Area	VD
Add security area	Security Area	C
Change properties of a security area	Security Area	VW
Link security area to security profile	Security Area Security Profile	V VW
Define default security areas	Security Area	VP
Turn Area Support on or off (global)	Area	P

Tasks on Class Permissions

The following table gives details of tasks on class permissions, security class the tasks belong to, and the corresponding permission required on these classes.

Task	Security Class	Permissions
General GUI access	Domain Security Profile	VR V
Show class permissions	Class Permissions	VR
Change class permissions	Class Permissions	VRP

General Security Tasks on Secured Objects

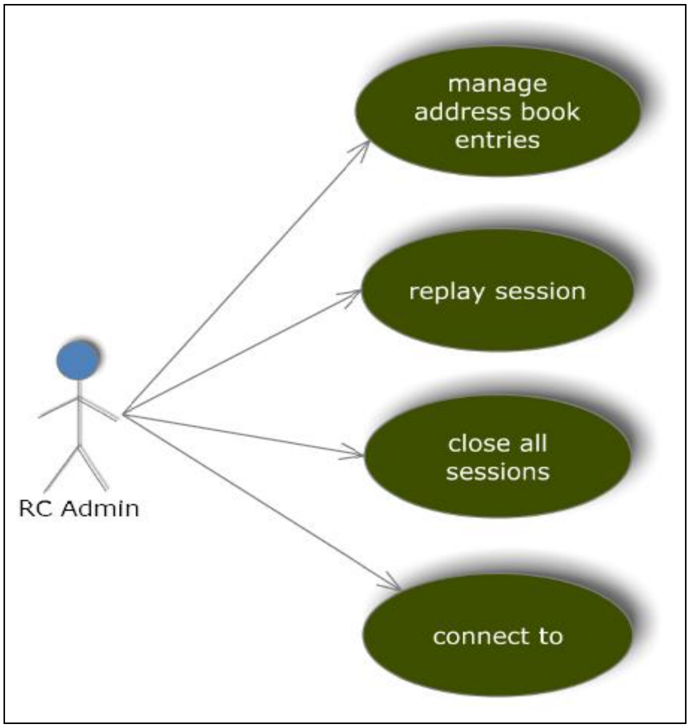
The following table gives details of tasks, security class the tasks belong to, and the corresponding permission required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Show group or object permissions	<Object Class>	VR

Task	Security Class	Permissions
	Security Profile	V
Change group or object permissions	<Object Class> Security Profile	VRP V
Link object to security area	<Object Class> Security Area	VRP V
Revert security level of security area	<Object Class> Security Area	VRP V
Take object ownership	<Object Class>	VRO

Remote Control Use Cases

The following illustration shows the use cases to set up and customize the remote control settings in an existing CA ITCM environment.



Actors

The actor for the remote control use cases, and his or her scope is as given below:

RC Admin

Responsible for managing assets via remote control.

Tasks on Remote Control

The following table gives details of tasks on remote control, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Enable remote control usage	Control Panel Access Remote Control Access	R V

Permissions for Remote Control Access

The following permissions are available for remote control access:

Create (C)

This permission is not used.

View (V)

View permission is required to make the Remote Control Node visible in the domain tree, under group details, and computer.

View permission is required to send commands to RC agents (Lock, Unlock, Reboot). You have to set the Write permissions on the computer or the group object to allow sending commands.

Read (R)

This permission is not used.

Delete (D)

Lets you delete user permission from a group.

Execute (X)

This permission is not used.

Write (W)

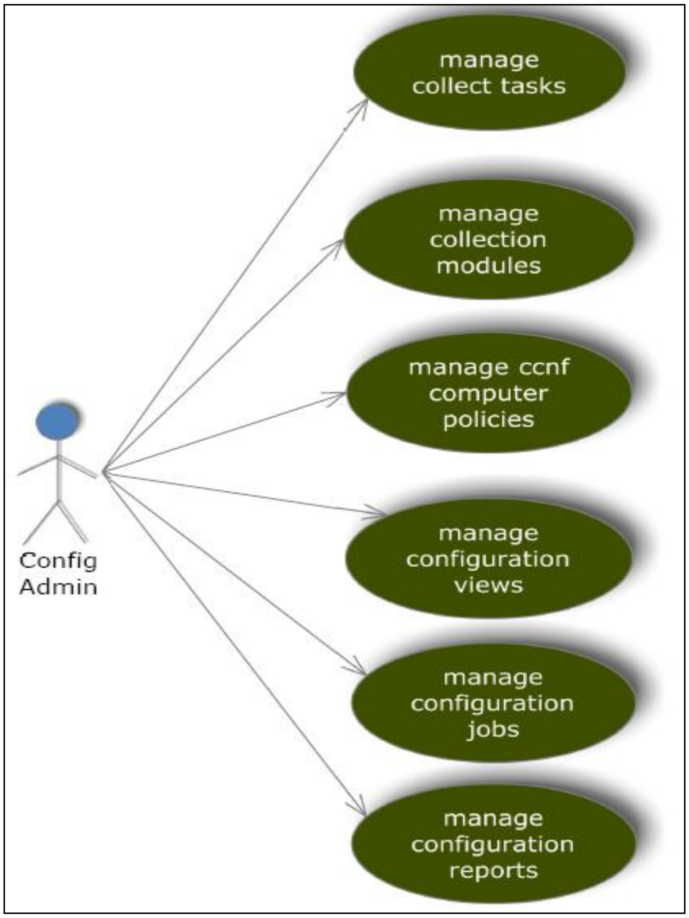
Lets you add user permissions to a group.

You require the Write permission on a Group object before you can add RC Permissions to it. To set permissions on the Root Global Address Book, you require the Write permission on the domain class.

Note: The Delete and Write permissions are *not* used in r11.2.

Configuration Use Cases

The following illustration shows the use cases to configure the CA ITCM environment.


manage collect tasks
manage collection modules
manage ccnf computer policies
manage configuration views
manage configuration jobs
manage configuration reports
Config Admin

Actors

The actor for the configuration use cases, and his or her scope is as given below:

Configuration Administrator

Responsible for configuring CA ITCM infrastructure and its assets.

Tasks on Collection Tasks

The following table gives details of tasks, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR

Task	Security Class	Permissions
Create a Collect Task folder	Control Panel Access	VR
Delete Collect Task folder	Control Panel Access	VR
Rename Collect Task folder	Control Panel Access	VR
Create a collect task	Control Panel Access	VR
Delete a collect task	Control Panel Access	VR
Set scheduling on a collect task	Control Panel Access	VR
Modify properties on a collect task	Control Panel Access	VR
Set permissions on a collect task	Control Panel Access	VR

Tasks on Collection Modules

The following table gives details of tasks on Collection modules, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR

Tasks on Configuration Policies

The following table gives details of tasks on configuration policies, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Configuration policy folder access	Control Panel	VR
List configuration policies	Policy-Configuration Computer	V
Browse configuration policies	Policy-Configuration Computer	VR
Create configuration policies	Policy-Configuration Computer	C
Modify configuration policies	Policy-Configuration Computer	W
Delete configuration policies	Policy-Configuration Computer	D

Tasks on Configuration Views

Configuration views are not subject to security.

Tasks on Configuration Jobs

The following table gives details of tasks, security classes the tasks belong to, and the corresponding permissions required on these classes.

Task	Security Class	Permissions
General GUI access	Domain	VR
Configuration policy folder access	Control Panel	VR
Configuration policy access	Policy-Configuration Computer	V
Create or delete computer configuration job	Computer	VRX
Create or delete group configuration job	Asset Group	VRX
View computer configuration job	Computer	VR
View group configuration job	Asset Group	VR

Tasks on Configuration Reports

The following table gives details of tasks on configuration reports, security classes the tasks belong to, and the corresponding permissions required on these classes.

Tasks	Security Class	Permissions
General GUI access	Domain	VR
View configuration report	Computer	VR
Request configuration report	Computer	VRX

Chapter 4: Scenarios

This section has examples of best practice recommendations for setting up Authorization in your CA ITCM environment.

Allow Software Delivery for Single User

This scenario demonstrates the security concept of software delivery tasks.

You can grant permissions for a user to create, edit, and distribute software for a specific group of computers, while you can deny these permissions to other users. You can create one or more user groups, thus creating independent islands of sub-administrators.

To grant permissions to users

1. Open the Security Profiles dialog.

   Reserve the Administrators group for users with more extensive privileges.

   Note: Do not make changes to the Everyone and Owner/creator groups.

2. Create a new security profile, USER1 (a user account) that will have restricted usage.

3. Use the Administrator group and set the class permissions for this profile as shown in the following table:

Object Class	Class Permissions	Comments
Software Package	Special Access (C)	Creates the software package. No other rights are required as you are the owner of the software package after you create it.
Procedure	Special Access (C)	Creates a procedure.
Software Job	Special Access (C)	Creates a software job on the target computer.
Software Job Container	Special Access (CVRW)	Creates, writes, and views the job container. This is available under the Jobs, Software Jobs, and All Software Jobs folders.
All Other Object Classes	No Access	Restricts a user from accessing other objects.

Allow Linking of Engine Jobs

You can allow users to link engine tasks to an engine.

To allow a user to link engine tasks to an engine

1. Create a new security profile, USER1 (a user account), that will have restricted usage.

2. Set the class permissions for this profile as shown in the following table, using the Administrator group:

Object Class	Class Permissions	Comments
Engine	<Change>	■ To start, stop, or modify engine objects, you must grant Full Control rights to the engine. ■ Requires NT Administrator or root rights to the computer where the engine is running.
Engine Task	<Manage>	

Use Area Support

You can have two or more profiles where all security profiles have the same class level permissions. However, objects created by one profile should not be seen by the other profiles.

To use area support

1. Log on as a user with Security Admin permissions.

2. Set up the requested security profile including the class permissions.

3. Create an area definition for each security profile.

4. Enable area support at the global level.

5. Enable area support for each security profile.

6. Link a security profile to a single area. Ensure that the each security profile is linked to a different area.

Note: A maximum of 32 area definitions are supported.

Allow Software Delivery for Certain Objects

You can have two Software Delivery Admin groups to create Computer groups, but the Software Jobs created by one Software Delivery Admin group should not be visible to other groups.

To allow software delivery for certain objects

1. Log on as a user with Security Admin permissions.
2. Create a security profile for each Security Admin group.
3. Assign the same class level permissions for each group allowing Software Delivery features.
4. Create an area for each Software Delivery Admin group.
5. Link the security profile for each Software Admin group to a different area.
6. Enable area support at global level.
7. Enable area support for each security profile.

Restrict Permissions for Administrator Profile

You can restrict the permissions for the Administrator profile.

To restrict permissions for the Administrator profile

1. Log on as a user with Security Admin permissions.
2. Modify the class permissions for the profile according to the requested restrictions.
3. Ensure someone or another security role will be able to modify permissions when you make this change.

You do not want to restrict all users and all roles from being able to modify permissions when you make this change.

Restrict Access for Local Administrator Group

During installation, CA ITCM creates a security profile for the local administrator group with Full Access rights.

You can restrict the permissions for the local administrator group.

To restrict permissions for the local administrator group

1. Create a new security profile for a user or a user group which has full access.
2. Restrict the permissions for the local administrator profile. For example, you may give only read and view permissions for all security classes.

Chapter 5: Performance Considerations

Consider the following points when setting up the object-level security (OLS) environment:

- The number of security profiles has a significant impact on the performance of the OLS environment.
- When you create a security profile, the permissions for all existing secured objects are calculated and stored in the MDB.
- The number of dynamic groups has a significant impact.
- The Engine, which runs in the background, evaluates the dynamic groups. Every time a dynamic group is evaluated, the permissions for the group members are updated or recreated.

The following scenario describes the impact of these considerations.

Scenario: Multiple Security Profiles and Dynamic Groups

Pre-Condition

A CA ITCM administrator creates 20 security profiles and more than 20 dynamic groups. There is one extra engine for group evaluation.

Action

The CA ITCM administrator creates an additional security profile using DSM Explorer. The administrator has also executed a group evaluation process.

Result

The CA ITCM administrator receives an error message saying the command timed out and the security profile was not created.

Root Cause

The creation of the security profile and the evaluation of the group are running in parallel; both processes access the same table when accessing the MDB table where the permissions are stored.

Solution

1. Stop the engine that is responsible for group evaluation.
2. Create the security profile.
3. Start the engine again to resume the group evaluation when the security profile create is completed.

   You can reschedule, postpone, or even disable the group evaluation of the engine until the security profile is created.

Security Classes Reference

Each security profile has its own set of security classes. A security class allows setting the permissions that will be assigned to an instance of such a class as soon as it is created.

CA ITCM supports the following security classes:

- Discovered Hardware (Computer)
- Class Level Security

Discovered Hardware (Computer)

The following security classes are used for Discovered Hardware only:

- Users
- Computer Users
- Manager
- Servers
- Asset Groups
- Server Groups
- Domain Groups
- Queries
- Security Classes
- Security Profiles
- Software Packages
- Software Procedures
- Procedure Groups
- Job Containers
- Software Jobs
- Asset Jobs
- Modules
- Query Based Polices
- Event Based Policies
- OSIM Boot Images
- OSIM OS Images
- Engine
- Configuration Policies Computer
- Configuration Policies User
- External Directory Access

- Report Templates
- Inventory modules

Class Level Security

Every object or instance of a class will get the permission as defined for the class by default.

The following security classes are used for Class Level only:

- MDB Access
- Enable Control Panel
- Enable Remote Control

Index