Enterprise Dynamic Access Control (EDAC)

Point of Contact:
Richard Fernandez
fernandr@spawar.navy.mil

Approved for public release; distribution is unlimited.
For licensing information contact:
Stephen Lieberman
Voice: (619) 553-2778
Mobile: (619) 606-5940
Email: stephen.lieberman@navy.mil

For comments regarding this product contact:
Richard Fernandez
Voice: (808) 474-9270
Email: richard.r.fernandez@navy.mil

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
Outline

Access control background
Access control lists
Groups
NIST RBAC standard

SEAC RBAC
Customer furnished and maintained assets
How it works
Product overview
Interoperability

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
Access Control Lists (ACL)

User name or unique identifier associates access to resources

![Diagram showing access control lists for Project Tracker](image)

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
User associated to a group and group associated to resources

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
Essentials for resource access

Necessary requirement to access resources:

• Not a user name
• Not a unique identifier
• Not a group association

• List of user characteristics
What are user characteristics

User characteristics (user profile)

• Where client works: **organization**
• What security credentials: **clearance**
• What pay category: **pay grade**
• What branch: **service**
• What vocation: **job function**
• etc
Examples of User Profiles

• User profile is a unique list of user characteristics.
• A client may have more than one user profile.
• User attributes should be compiled from an authoritative data source(s) on a real-time basis.

<table>
<thead>
<tr>
<th>Categories</th>
<th>COMPACFLT</th>
<th>USNR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Organization:</td>
<td>CPF N65</td>
<td>Naval Intel</td>
</tr>
<tr>
<td>Clearance:</td>
<td>Secret</td>
<td>Top Secret</td>
</tr>
<tr>
<td>Paygrade:</td>
<td>DP3</td>
<td>02</td>
</tr>
<tr>
<td>Service:</td>
<td>DoD</td>
<td>DoNR</td>
</tr>
<tr>
<td>Function:</td>
<td>Program Manager</td>
<td>Intelligence</td>
</tr>
</tbody>
</table>

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
Impact on resource access

The following can affect resource access:

• Transfer to another organization
• Loss of security clearance
• Change in job title
• Job promotion

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
Problems with ACLs and Groups

Maintaining an updated ACL or group is time consuming.

Situation worsens when:

• Number of users increase
• Number of resources increase

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
NIST RBAC compliance

Because of ACL and group limitations:

The National Institute of Standards and Technology (NIST) RBAC is an American National Standard - ANSI INCITS 359-2004 (approved 19 Feb 04)
Definitions:

**Users and Roles:** “…access decisions are based on the roles that individual users have as part of an organization. “Access rights are grouped by role name…”

**Role hierarchies:** "Under RBAC, roles can have overlapping responsibilities and privileges;"

**Roles and Operations:** "Organizations can establish the rules for the association of operations with roles."
Access control comparison

How access control solutions can simultaneously evaluate user characteristics.

<table>
<thead>
<tr>
<th>ACLs</th>
<th>Simultaneous evaluation of multiple object characteristics &amp; environmental</th>
<th>Simultaneous evaluation of multiple object characteristic &amp; environmental</th>
<th>Real-time detection of object characteristic changes, thus affecting resource access</th>
</tr>
</thead>
<tbody>
<tr>
<td>Groups</td>
<td>0</td>
<td>No</td>
<td>No</td>
</tr>
<tr>
<td>EDAC</td>
<td>Unlimited</td>
<td>Yes</td>
<td>Yes</td>
</tr>
</tbody>
</table>
Customer meta-database background

Relational database data duplicated on a directory service.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
Customer meta-database specifications

- Customer meta-database
- LDAP v3/DSML directory
- X500 class objects
  - organization
  - organizationalUnit
- Scalable
  - unlimited entries
  - modifications allowed
- Structure designation
  - domain
  - reference category
  - values
- Structure
  - flat
  - hierarchal
- Maintained
  - local commands
  - regional commands

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
Customer meta-database domain

Domain consist of global and regional directories.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
User selects a profile to determine resource access. Mgmt constraints on user profile selections

User Profile Manager service

SPAWAR Profile
- clearance: secret
- organization: engineering
- billettitle: project manager
- paygrade: GS13

COMPACFLT Profile
- clearance: top secret
- organization: engineering
- billettitle: developer
- paygrade: GS13

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
How the EDAC works

Step 1:
Resource manager establishes a set of conditions to access a resource.

These set of conditions represent a resource profile.

RBAC Condition Manager

Customer Meta-Database

Resource Profile
ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

RBAC Resource Directory

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
How the EDAC works

Step 2:
An effective RBAC requires real-time creation of user profile(s) from authoritative data source(s).

Customer Multiphase Database

Structure Format Service

Customer Personnel Database

Reference Categories
- assignedCommand
- clearance
- paygrade

Attributes
- Secret
- GS3
- N65

User Profile
- ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
- ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise
- ou=GS3, ou=GS2, ou=GS1, ou=Paygrade, o=Enterprise

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
How the EDAC works

Step 3:
The RBAC Rules Engine compares User and Resource Profiles to determine resource access.

User Profile
ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise
ou=GS3, ou=GS2, ou=GS1, ou=Paygrade, o=Enterprise

Customer Resource Database
- Project Tracker (resource)
- HR Service (resource)
- Payroll Application (resource)

Repository Service

Project Tracker Resource Profile
✓ ou=N65, ou=N6, ou=CPF, ou=assignedCommand, o=CPF
✓ ou=secret, ou=confidential, ou=fouo, ou=clearance, o=Enterprise

The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.
<table>
<thead>
<tr>
<th>Resource Roles for Project Tracker</th>
<th>Resource Profiles</th>
</tr>
</thead>
<tbody>
<tr>
<td>Guest</td>
<td>CPF Guest</td>
</tr>
<tr>
<td></td>
<td>T COMPACFLT</td>
</tr>
<tr>
<td></td>
<td>T CSP Guest</td>
</tr>
<tr>
<td></td>
<td>T DoD</td>
</tr>
<tr>
<td></td>
<td>T CNR Guests</td>
</tr>
<tr>
<td></td>
<td>T COMNAVREG</td>
</tr>
<tr>
<td></td>
<td>। Tuesdays 1700-2300</td>
</tr>
<tr>
<td>User</td>
<td>CPF N8 Users</td>
</tr>
<tr>
<td></td>
<td>T CPF N6</td>
</tr>
<tr>
<td></td>
<td>T GS12</td>
</tr>
<tr>
<td></td>
<td>। Mon &amp; Thurs 0800-1300</td>
</tr>
<tr>
<td>Administrator</td>
<td>CPF Admin</td>
</tr>
<tr>
<td></td>
<td>T CPF N65</td>
</tr>
<tr>
<td></td>
<td>T TS</td>
</tr>
<tr>
<td></td>
<td>। Mon &amp; Thurs 0800-1300</td>
</tr>
<tr>
<td></td>
<td>Deny CPF N6 Admin</td>
</tr>
<tr>
<td></td>
<td>T CPF N65</td>
</tr>
<tr>
<td></td>
<td>T CONTR</td>
</tr>
</tbody>
</table>

- Resource roles
- Allow & Deny profiles
- Exact and subtree conditions
- Time constraints

*The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.*
The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.
EDAC – Security levels

During INFOCON B

During INFOCON C

- Pre-configure conditions under each security level.
- RBAC Rules Engine evaluates only conditions for prevailing security level.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
EDAC – Model

EDAC standard initiative:

• Interchangeable modular access control components
• Minimum salient features
• Protocol between components
• Standard tie-ins between customer assets and access control system
EDAC - Model

EDAC Process
(A) Administrative Service - establishes resource containers, CMD referrals, RM accounts.

Repository Service

A1

Administrative Service

Customer furnished and maintained assets

Enterprise Dynamic Access Control (EDAC)

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
EDAC - Model

EDAC Process
(B) Condition manager Service - Establishes and edits conditions to access resources.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.

EDAC Process
(D) Customer Environmental Interface - furnishes environmental updates.
The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.
The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.
EDAC interoperable among regions:

• Set conditional access for remote users
• Domain customer meta-databases
Pearl Harbor: resource profile created for local resource access.

The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.
Pearl Harbor: local user profile is generated to access a local resource.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
Pearl Harbor: user and resource profiles are evaluated by rules engine to determine local resource access.
EDAC - Interoperability

Pearl Harbor: A resource profile to allow remote users access to local resources.

*The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.*
EDAC - Interoperability

San Diego: user profile generated.

Resource Profile SD
SD N651
Top Secret
GS12

Condition Manager Interface

Enterprise customer meta-database

San Diego customer meta-database

SD User Profile
SD N651
Top Secret
GS12
Developer

Pearl Harbor

DoD

San Diego

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
EDAC - Interoperability

Pearl Harbor: San Diego user evaluated for Pearl Harbor resource access.

Resource Profile SD
SD N651
Top Secret
GS12
Developer

Condition Manager Interface

Enterprise customer meta-database

Pearl Harbor RBAC

Pearl Harbor

Customer resources

DoD

San Diego

SD User Profile
SD N651
Top Secret
GS12
Developer

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
EDAC - Interoperability

San Diego: same user evaluated for San Diego resource access.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."
The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.
"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

San Diego, CA 92152-5001
Approved for public release; distribution is unlimited.