DEPARTMENT OF THE NAVY
HEADQUARTERS UNITED STATES MARINE CORPS
3000 MARINE CORPS PENTAGON
WASHINGTON, DC 20350 3000

IN REPLY REFER TO
5231
IC4
APR 15 2022

From: Director, Information Command, Control, Communications, and Computers
To: Distribution List

Subj: ENTERPRISE SERVICE ROLES, RESPONSIBILITIES, AND PERMISSIONS GUIDE

Ref: (a) IRM-5271-01
(b) MCO 5271.1B

Encl: (1) Information Resources Management (IRM) 5231-01D Version 4.5 Enterprise

1. Purpose. To update and outline the technical security roles and responsibilities for supporting regionally hosted Marine Corps Enterprise Services. This document defines standard and recommended access control entries on Active Directory integrated and Non-Active Directory integrated enterprise systems. This guide includes the Marine Corps Enterprise Network (MCEN) Active Directory Organizational Unit structure and permissions and is applicable to both classified and unclassified Enterprise Services.

2. Cancellation. This IRM 5231-01D version 4.5 effectively cancels all previous IRM 5231-01 documents. In order to remain current on emerging technologies and programs across the MCEN, this document will be reviewed every twelve months and updated accordingly.

3. Authority. The information promulgated in this publication is based upon policy and guidance contained in the references.

4. Applicability. This publication is applicable to the entire Marine Corps.

5. Scope

a. Compliance. Compliance with the provisions of this publication is required unless a specific waiver is requested.

b. Waivers. Waivers to the provisions is this publication will be authorized by the Commanding General, Marine Forces Cyberspace Command.

6. Sponsor. The sponsor of this technical publication is Deputy Commandant for Information, Command, Control, Communications, and Computers.

J. A. MATOS

DISTRIBUTION STATEMENT A: Approved For public release; distribution is unlimited.
DISTRIBUTION: PCN 18623001700

MARINE CORPS INFORMATION RESOURCES MANAGEMENT (IRM) 5231-01

ENTERPRISE SERVICE ROLES, RESPONSIBILITIES, AND PERMISSIONS GUIDE

March 31, 2022

Version 4.5

Revision History

Document Revision #	Date	Revision Made By	Description of Revisions	Pg #
1.0	August 2011	HQMC C4/CP	Signed Initial Release	
2.0	November 2015	Jim Calvin	Updates throughout, including expansion of tactical	
2.1	August 2016	Maj Shannon Clancy	Updates to all	All
2.1	August 2016	Jim Calvin	Comments / review	All
2.2	February 2017	Jim Calvin	Updated MCNOSC references to MCCOG	All
2.3	January 2018	Jim Calvin	Added Service Accounts section	
2.3.1	8 June 2018	Capt Aaron Mora	Added to Tactical-Extensions	
2.4	19 June 2018	Maj Joni Ong	Updates to all from DON Tracker CRM	All
3.0	31 July 2018	Jeff Hunter	Signed Release	
4.0	06 August 2021	Jeff Hunter	Updated with MCCOG/MFCC Input	All
4.1	14 October 2021	Jeff Hunter	Updated following DON Tasker Review	All
4.2	22 October 2021	Maj Joseph Russell	Updated ADFS permissions, modified KMS to reflect new ADBA	8
4.3	08 November 2021	Jeff Hunter	Updated Permissions Table to reflect comments from MCICOM	9 (Table)
4.4	18 March 2022	Jeff Hunter	Updated following DON Tasker GO Review	All
4.5	23 March 2022	Maj Joseph Russell	Updated MEMS Permissions for FMF	13 (Table)

Table of Contents

1. Introduction

In order to maintain cybersecurity and information dominance, the Marine Corps must provide an information environment that is both secure and supportive of operational requirements. This balance for Directory Services is achieved through the management and maintenance of the Active Directory (AD) Forests and Domains supporting Marine Corps applications, users, and devices. Permissions (user and administrative) and the AD Organizational Unit (OU) structure are critical elements that enable effective management and security of systems. The Marine Corps Strategy for Assured Command and Control, published in March 2017, states that Marine Corps Command and Control (C2) is best realized via an “interoperable and resilient MCEN.” The Marine Corps Enterprise Network (MCEN) is the Marine Corps’ network of networks and approved interconnected network segments. It comprises people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations. Furthermore, the MCEN incorporates elements of:

- Operations and maintenance functions that provision data transportation, enterprise services, network services, and boundary defense
- Programs of Record that provide network services to forward deployed forces

In this document, regional refers to the Marine Corps Installations Command (MCICOM) and Marine Forces Cyber Command (MFCC) entities that operate and defend the network until it is superseded by revised or updated documentation. These services and capabilities are broken down into three main categories:

- Security/Network Assurance
- Enterprise
- Regional/Local

This guide addresses enterprise services in support of garrison and deployed environments. Enterprise services are those provided, operated, and maintained by the Marine Corps Cyberspace Operations Group (MCCOG). Generally, enterprise services are the common physical/virtual infrastructure, applications, and services operated and managed in support of all users and organizations across the Marine Corps. This enterprise implementation provides a dependable, robust, and secure communication backbone that includes high availability/disaster recovery and supports missions across the Marine Corps.

2. Purpose

The purpose of this document is to provide the overarching guidance for enterprise roles, responsibilities, and permissions as they pertain to the operations and maintenance roles and responsibilities for supporting regionally hosted Marine Corps enterprise services. This document also defines standard (required) and situationally dependent access control entries on AD/AD-integrated and non-AD integrated systems in support of the following core services:

- Identity
- Access Management
- Collaboration
- Data Management

Operating enterprise services without aligning permission assignments to directly support roles and functions increases risk to the MCEN. Clarifying the responsibilities for each organization and defining clear boundaries improves the security posture and minimizes impact to services caused by change (particularly incorrect change caused either by human error or malicious intent). While protecting the information environment, the permission delegation identified in this guide also empowers MFCC, MCICOM, Fleet Marine Forces (FMF), and Programs of Record to deliver the highest level of support to end users.

Security principles highlighted through this guide include:

- **Least Privilege** – Grant administrators only the permissions required to perform their duties.
- **Decentralized Administration** – Position most administrative activity as close to the end user as possible for faster, more accurate resolution of issues.
- **Tiered Administration** – Establish a supporting chain of administrators for issue escalation that narrows to the engineers of the solution, including centralized vendor support.
- **Role Based Administration** – The permissions model is designed to be aligned to administrative functions instead of individual users in order to ease the establishment and maintenance of security groups.
- **Ease of Use** – Automated operations and reporting.
- **Auditing** – Provide oversight of administrative procedures in order to increase transparency and efficiency.
- **Standardization** – Issue permissions and conduct activities in the same manner across regional and administrative boundaries throughout MCEN and Deployed Marine Corps Enterprise Network (DMCEN) environments enabling support to users and objects within respective areas of operations and responsibility.

3. Active Directory Methodology

As a key element of MCEN unification, AD logical structure on the Secret Internet Protocol Router Network (SIPRNet), Marine Corps Worldwide (MCW) and Non-Secure Internet Protocol Router Network (NIPRNet) Marine Corps Directory Service (MCDS) forests have been restructured to support regionalization requirements. In order to ensure permissions can be delegated securely, and with the most flexibility to respond to mission requirements, security groups and nesting are being leveraged as the foundation.

Groups have been created at each OU administrative level to support AD logical administration and to lay a framework to facilitate administration of AD-aware services, such as Exchange or SharePoint.

At the core of the enterprise, MCCOG is responsible for ensuring the uninterrupted delivery of directory services worldwide. This includes, but is not limited to, the following administrative tasks:

- Adding and removing domain controllers
- Managing and monitoring replication
- Ensuring the proper assignment and configuration of operations master roles
- Ensuring the recoverability of the directory services databases
- Managing domain and domain controller security policies
- Configuring directory service parameters, such as setting the functional level of a forest
- Defining and linking Group Policy Objects (GPOs) for the enterprise

In the MCEN environment, user support is provided based on geographic location and the C2 reporting structure established in accordance with (IAW) MCO 3100.4A, Cyberspace Operations. MFCC is responsible for managing the content that is stored and protected by AD and non-AD enterprise systems. Permissions for the management and use of enterprise systems are identified within Appendix A of this guide and shall be granted accordingly. Data management tasks include, but are not limited to, managing the following content:

- Cyber Security Services
- End User Services
- Application Services
- Identity and Authorization Services
- Software Delivery
- Public Key Infrastructure (PKI)
- System Infrastructure
- Unified Communications
- Local Hosted Services

The MFCC, or enterprise tier, provides appropriate levels of permissions to manage the users, computers, and data within the MCCOG (including all MCCOG Detachments), and Network Battalions/Network Activities within their respective regions. This tier includes MCCOG, MAGTF (Marine Air-Ground Task Force) Information Technology Support Center (MITSC), and USMC Enterprise OUs. Administrators within these OUs have their system access and authorization requests vetted by the MCCOG.

- **USMC** – The top-level OU within the AD, which houses non-default AD objects, domain controllers, and contacts.
- **MFCC -**– Directly under the USMC OU, this tier provides appropriate levels of permissions to manage the users, computers, and data within their respective regions. Administrators within this OU have their system access and authorization requests vetted by the MCCOG.
- **Base/Post/Stations (B/P/S)** – Specific to each region, these OUs fall under MFCC, and permissions are delegated by appropriate Network Battalions/Activities in order to support mission requirements.
- **Tenant/Supported Commands (T/SC)** – Specific to each region, these OUs fall under MFCC; permissions are delegated by appropriate network battalions and activities in order to support mission requirements.
- **Programs of Record** (**POR) –** OUs created under the USMC root containment systems that should be patched in accordance with approved Authorization to Operate/Authorization to Connect (ATO/ATC), accept default security policies, or be managed in the same manner as baseline MCEN systems. POR OUs sit at the Enterprise level but have differing permissions to affect their respective objects and required administration.
- **Tactical-Extensions (TE)** – Tactical Extension OUs are in place to support the FMF. These reside at the Enterprise local service level and are intended to enable deployed users with permissions needed to support mission requirements.
- **USMC Enterprise Administration** – This folder is specific to Forest level administrative activity and is populated by a restricted number of MCCOG administrators only.
- **USMC Enterprise Servers** – This folder supports those servers performing enterprise service functions and is managed and maintained by MCCOG administrators.

4. Considerations

Windows Credential Theft Mitigation

Windows credential theft is a technique in which an attacker initially gains highest privilege (root, Administrator, or System, depending on the OS) access to a computer on a network and then uses freely available tools to extract credentials from sessions of other active accounts. The goal of this type of attack is to gain credentials of privileged (administrator) or “Very Important Person” (VIP) accounts. Compromise of either type of credential poses a threat/risk to operations within the MCEN.

In order to counter this risk, several mitigating actions have been implemented. Role-based permission models have been established to align with industry best practice to support mission requirements at the lowest level. Administrators must request specific role- based permissions and use required tools, via Utility servers, to provide data management and administration within their designated area of responsibility. Appendix C illustrates use cases for each administrative activity; these are also further defined in the Utility Server Design (Appendix C, reference P).

Account/Object Retention

Dormant user objects/accounts within AD can serve as a gateway for attackers to access the Marine Corps information environment. Data and licensing resources are taxed by maintaining these accounts on the MCEN. For these reasons, it is critical that established policy is followed relating to dormant account management and maintenance. AD administrators shall adhere to guidance identified within MARFORCYBER FRAGO 008 and ECSM 007 (Appendix C) for account disabling and/or deactivation. Accounts/objects that were disabled will remain within the AD OU until automated data retention policies are implemented.

Service Accounts

Service accounts are AD user objects or Group Managed Service Account objects that have been created within AD and placed in a specific OU based on the administrative tier that is responsible for its management. Service accounts facilitate the execution of a service process on a computer that requires certain permissions. Service accounts must have an associated account owner or custodian. Requestors of service accounts must provide a point of contact when requesting the account. Services use the service accounts to log on and make changes to the OS or configuration. Service accounts are critical to the management of a particular service and must be established within the appropriate AD OUs (i.e., T/SC and Tactical Extension OUs to support DMCEN operations) for continuous operations and management of services. IAW Appendix A, only MCCOG has the responsibility to create and manage service accounts.

In adherence with the MFCC requirement to strengthen identity and access management practices, the requirement for service accounts must follow a stringent process. Service accounts are placed in two groups upon creation: one that prevents them from being Smart Card enforced for interactive log-on, and one that denies them interactive log-on on Windows operating systems in the unified forest.

For a service account to have value, it must belong to one or more control groups so that it can accomplish the set of tasks enabled by that membership. The application/service owner is responsible for identifying the set of tasks that a service account must be allowed to execute. Service accounts must adhere to existing FRAGO and STIG requirements, must be registered in the application/service delegated permissions model, and must use the MCEN Naming Standard for Application and Systems (Appendix C, reference L) in the construction of their names.

Tactical Extensions Organizational Unit

The Tactical-Extensions OU structure identified within AD will allow Commanders to deploy essential Enterprise services and information resources without the need to establish tactical domains and create new user identities. This concept is described in the DMCEN COE (Appendix C, reference A) signed in 2017.

Programs of Record Organizational Unit

PORs are those systems or applications that are not operated and maintained but are supported by the MCCOG. In general, PORs are systems and applications that are not enterprise services or systems such as MCEN end user devices. PORs may be AD integrated; however, system configurations are maintained by acquisition commands such as Marine Corps Systems Command or NAVAIR. As depicted within Appendix A, POR objects that are AD integrated will be located within POR OUs that are in the same tier/level as the Network Battalions/Network Activities since PORs have unique requirements that, in some cases, will not allow full functionality if standard enterprise security policies and settings are applied. Additionally, the administration of POR objects may differ from "standard" user and computer objects. The POR Playbook, Appendix C, reference F, further identifies the process for AD OU creation, group policy implementation and the modification process, as well as other requirements to operate on the MCEN.

5. Roles and Responsibilities

Roles and responsibilities outlined within this section are further delineated within Appendix A. Appendix A specifically identifies the entities conducting operations and maintenance roles throughoutthe MCEN and the level of permissions provided to each role (tier/level) respective to each enterprise system.

MCCOG

MCCOG is accountable and responsible for the operations and maintenance of enterprise service equipment/infrastructure (excluding MCICOM-owned infrastructure) throughout the MCEN. They also maintain authority for MCEN AD OU structure and permissions delegation, as well as administering objects and their containers at the enterprise level. Management of AD objects supporting MARFORCYBER, Enterprise Service Desk, and MCCOG Detachments also fall under the MCCOG.

Network Battalion/Network Activity

Network Battalions/Network Activities are responsible for operations and maintenance functions of enterprise systems within their respective region as identified within Appendix A. Additionally, Network Battalions/Network Activities have the ability to support inherited functions down to the B/P/S and T/SC level as defined within Appendix A, and modify membership to subordinate OU security groups. Any escalation of support required shall be coordinated with the MCCOG.

Base/Post/Station (B/P/S)

Base/Station Commands are accountable and responsible for operations and maintenance functions of systems within their respective area or region as identified in Appendix A. Any escalation of support required shall be coordinated with their supporting Network Battalion/Network Activity.

Tenant/Supported Command (T/SC)

T/SCs are accountable and responsible for operations and maintenance functions of systems as identified in Appendix A. Tenant/Supported Commands may be FMF commands or other supporting establishment commands that fall within a Network Battalion/Network Activity and B/P/S's area of responsibility. Any escalation of support required shall be coordinated with their respective supporting B/P/S and/or Network Battalion/Network Activity. Permissions will be requested and granted as required by the Network Battalion/Network Activity.

Fleet Marine Forces (FMF)

FMF units are accountable and responsible for services within tactical extension OUs. These services are intended to provide Operational Commanders required support when operating in garrison and/or deployed environments.

Defensive Cyberspace Operations (DCO) Forces

DCO includes Cyberspace Protection Teams (CPTs), MCCOG DCO and DCO Internal Defensive Measures (IDM) companies serve as the quick reaction defensive force responding to network intrusions. DCO Forces may be required to have full control and at a minimum, read rights, to enterprise systems and applications. Permissions will be requested and granted as required via the MCCOG.

DCI IC4/CY ICE DEMon/White Team

The Marine Corps Institutional Cybersecurity Enterprise Defense Monitoring Team (ICE DEMon Team), also known as the "White Team," independently identifies and validates vulnerabilities on all systems and network devices in order to reduce the overall risk to the MCEN. In order to perform vulnerability assessment activities on a continuous basis, the White Team requires sufficient access to perform vulnerability assessments or compliance validations, on all MCEN information systems. Specific permissions or access may vary (based on individual system or application) and can range from audit-level to administrative-level access. System/application access is authorized under the authorities of the Marine Corps Chief Information Officer (CIO), Senior Information Security Officer (SISO), or Authorizing Official (AO) and granted via the MCCOG.

POR

POR managers are accountable and responsible for operations and maintenance functions of POR systems as identified in Appendix A in their respective area of responsibility/region and IAW the

POR Playbook (Appendix C, reference F). Permissions will be requested and granted as required based on location or tier in active directory (MCCOG/Network Battalion/Network Activity/FMF).

Appendix A. Enterprise Permissions

The following permissions are assigned in order to enable organizations to execute the roles and responsibilities as identified within the MCEN C2 MROC Decision Memorandum. The delegation of permissions has been designed to allow maximum flexibility within all organizations while maintaining a defensive and secure posture for the enterprise. Permissions identified within the RASCI chart are codified in support and control security groups and defined within each system's delegated permissions model. This Appendix will be updated as enterprise technologies andservices are added or decommissioned throughout the MCEN.

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
ACAS								
Administer Security Center servers	F		R				R	R
Administer Security Center servers on Tactical Extensions	F		F				R	R
Administer Nessus Scanner servers	F		R				R	R
Administer Nessus Scanner servers on Tactical Extensions	F		F				R	R
Administer Security Center application	F		R				R	R
Administer Security Center application on Tactical Extensions	F		F				R	R
Run scans scoped to the enterprise	W						R	M
Run scans scoped to the Net Bn/Act	*	M	R				W	M
Run scans scoped to the Tactical Extensions	*		M				W	M
Run scans scoped to the B/P/S	*	*		M			*	M
Run scans scoped to the T/SC	*	*		*	M		*	M
Run scans scoped to the PoR	*		M			M	*	M
Active Directory Based Activation								
Obtain licenses from MCSELMS	F		F					R
Administer ADBA servers	F		R					R
ADFS								
Add ADFS Server to Farm	F						R	R
Add WAP Server to Farm	F						R	R
Add / Change Claims Provider	F	R	R				R	R
Add / Change Replying Party Trust	F	R	R				R	R
Update Certificates	F						R	R

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
AZURE AUTOMATION								
Develop Automation Tasks	F	M	M		M	M	R	R
Manage Azure Automation RBAC	F	M	M		M	M	R	R
BES								
Administer BES Server	F		R				R	R
Administer Devices & Users (See also Messaging)	F	M	M	W	W		R	R
Call Manager								
Administer Base/Post/Camp/Station Call Managers – MCICOM	R		R	F			R	R
Administer Enterprise Call Managers – MCCOG	F						R	R
Administer Tactical Entry Point Call Managers – MCCOG	F						R	R
Deploy Base/Post/Camp/Station Intercluster Trunks – MCICOM	F	M	R				R	R
Deploy Enterprise Intercluster Trunks – MCCOG	F	M	M				R	R
Deploy Tactical Entry Point Intercluster Trunks - MCCOG	F	M	M				R	R
Provision Base/Post/Camp/Station Telephones - MCICOM	F	M	M				R	R
Provision Enterprise Telephones-NetBn Provision Tactical Entry Point Telephones – FMF	F	M	M				R	R
Cisco ISE								
Administer ISE Appliance	F	R	R				R	R
Administer ISE Software Instance	F	R	R				R	R
Administer Account and Device Management	F	R	R				R	R
Desired State Configuration								
Administer DSC pull web server	F						R	R
Administer configuration Management Object Files (MOF)	F						R	R
Verify DSC implementation on enterprise servers	F						R	R
Verify DSC implementation on Net Bn/Act servers	*	M	R				R	R
Verify DSC implementation on Tactical Extension servers	*		M				R	R
Verify DSC implementation on B/P/S servers	*	*		M			R	R
Verify DSC implementation on T/SC servers	*	*	M	*	M		R	R
Verify DSC implementation on PoR servers	*	R	M		R	R	R	R

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
Dynamic Host Configuration Protocol Servers								
Administer DHCP servers at the Network Bn/Act level		F	R	R			R	R
Administer DHCP servers at the Tactical Extension			F				R	R
Distributed File System								
Administer DFS servers	F						R	R
Administer DFS namespace	F	M	M				R	R
Submit share UNC paths	*	F	M				R	R
Administer DFS replication groups	F	M	M				R	R
DNS - External								
Administer public DNS servers	F						R	
Administer public DNS zones	F						R	
DNS - Internal								
Administer internal standalone DNS servers	F	F	F			F	R	R
Administer domain controllers	F						R	R
Administer enterprise DNS zones	F						R	R
DMZ F5								
Administer F5 appliance	F	R	R				R	R
Audit F5 configuration and logs	F	R	R				R	R
Enterprise Boundary Base Firewall								
Administer MCEN Boundary	F	R	R	R	R	R	R	R
Forward Proxy								
Administer Forward Proxy application and server	F	R	R	R	R		R	R
Forward Proxy Reporter								
Administer BC Reporter	F		R				R	R
Run Reports BC Reporter	R	R	R	R	R		R	R
HBSS								
Administer, manage, and maintain MCEN HBSS servers	F	R	R				R	R

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
Administer, manage, and maintain MCEN HBSS servers within Tactical Extensions	*		F				R	R
Installs/maintains the HBSS point-products on the HBSS servers	F	R	R				R	R
Installs/maintains the HBSS point-products on the HBSS servers within Tactical Extensions	*		F				R	R
Create and maintain MCEN HBSS accounts	F	R	M				R	R
Administer permissions for MCEN HBSS accounts	F	R					R	R
Create and maintain MCEN HBSS policies	F	R	R				R	R
Implement HBSS modules and policies IAW policies and directives	F	R	R				R	R
Virus Scan Enterprise administration	F	R	R	R	R		R	R
Host Intrusion Prevention System (HIPS) administration	F	R	R	R	R		R	R
Rogue Systems Detection administration	F	R	R	R	R		R	R
Data Loss Prevention (DLP) administration	F	R	R	R	R		R	R
Policy Auditor (PA)	F	R	R	R	R		R	R
Asset Configuration and Compliance	F	R	R	R	R		R	R
Implement HBSS modules at the Net Bn/Act level	*	W	R	R	R		R	R
Implement HBSS modules at the Tactical Extension Level	*		M				R	R
Implement HBSS modules at the B/P/S level	*	*		W	R		R	R
Implement HBSS modules at the T/SC level	*	*		*	W		R	R
Administer top level organizational structure	F						R	R
Administer the organizational structure at Net Bn/Act level	*	M	R	R	R		R	R
Administer the organizational structure at Tactical Extension Level	*		M				R	R
Administer the organizational structure at B/P/S level	*	*	*	M	R		R	R
Administer the organizational structure T/SC level	*	*	*	*	M		R	R
Create, edit, view, run, and terminate Scheduler tasks	F	R	M	R	R		R	R
Patch and update HBSS servers	F		F				R	R
Identity and Access Management								
Administer root domain controllers	F						R	R
Administer child domain controllers	F	R	R				R	R
Administer organizational units	F	R	R	R	R	R	R	R
Administer leaf objects at Net Bn/Act level	*	F	R	R	R	R	R	R
Administer leaf objects at Tactical Extension Level	*	R	F	R	R	R	R	R
Administer leaf objects at B/P/S level	*	*		F	R	R	R	R
Administer leaf objects at T/SC level	*	*	F	*	F	R	R	R

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
Administer leaf objects at PR level	*	M	M	R	R	F	R	R
Administer leaf objects at Net Bn/Act level under PoR	*	F	M	R	R	*	R	R
Administer leaf objects at Tactical Extension Level under PoR	*	R	F	R	R	R	R	R
Administer group policy objects	F	R	M	R	R	R	R	R
Administer group policy links and link order	F	R	R	R	R	R	R	R
Administer forest FSMO roles	F	R	R	R	R	R	R	R
Administer domain FSMO roles	F	R	R	R	R	R	R	R
Administer AD Integrated DNS Zones	F							
Administer service accounts	F	R	M	R	R	R	R	R
Administer AD Physical Components	F	R	M	R	R	R	R	R
Administer AD Schema	F	R	R	R	R	R	R	R
Administer forest and domain trusts	F	R	R	R	R	R	R	R
Administer USMC Enterprise Servers leaf objects	F	R	R	R	R	R	R	R
Administer USMC Enterprise Administration leaf objects	F	R	R	R	R	R	R	R
IP Address Management								
Administer IPAM – Enterprise	F					R	R	R
Administer IPAM - Net Bn/Act	*	M	R			*	R	R
Administer IPAM - Tactical Extension Level	*		M			*	R	R
Administer IPAM - B/P/S	*	*	*	M		*	R	R
MEMS								
Administer MEMS services and servers	F						R	R
Manage end-user views (BSM)	F	M	M	M			R	R
Manage Operations Agent and policies (OMW)	F	R	R	R			R	R
Manage network device discovery (NNM)	F	R	R	R			R	R
Manage network device configuration (NA)	F	M	M	M			R	R
Manage Configuration Item collections (UCMDB)	F	R	R	R			R	R
Manage end-user access to web	F	R	R	R			R	R
Messaging								
Administer messaging services and servers	F	R		R	R		R	R
Administer organizational level configuration settings	F	R		R	R		R	R
Administer mailbox settings at Net Bn/Act level	*	M	M	R	R		R	R

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
Administer mailbox settings at Tactical Extension Level	*		M				R	R
Administer mailbox settings at B/P/S level	*	*	*	M	R		R	R
Administer mailbox settings at T/SC level	*	*	*	*	M		R	R
Administer distribution groups at Net Bn/Act level	*	M	R	R	R		R	R
Administer distribution groups at the Tactical Extension Level	*		M				R	R
Administer distribution groups at B/P/S level	*	*	*	M	R		R	R
Administer distribution groups at T/SC level	*	*	*	*	M		R	R
Administer global address list	F		*				R	R
Administer GFE handhelds at Net Bn/Act level (See also BES)	*	F	R				R	R
Administer GFE handhelds at the Tactical Extension Level	*		M				R	R
Administer GFE handhelds at B/P/S level (See also BES)	*		*	F			R	R
Administer GFE handhelds at T/SC level (See also BES)	*		*		F		R	R
NACCR								
Grants membership in local Administrators group on NACCR servers	F	R	R	R	R	M	R	R
Grants full control of NACCR Operations Manager application.	F	R	R	R	R	M	R	R
Grants members SysAdmin role within all NACCR databases.	F	R	R	R	R	M	R	R
OPDRS								
Administer OPDRS Users	F						R	R
Administer OPDRS Structure Hierarchy	F						R	R
Draft and Release Directives, Advisories, and MDTMs	F	R		R	R	R	R	R
Report Compliance	F	M	W	M	M	M	R	R
Manage POA&Ms	F	M	W	M	M	M	R	R
Administer Servers and Services	F						R	R
Administer Web Applications	F						R	R
Public Key Infrastructure								
Administer Certificate Authorities	F						R	R
Administer vCenter Servers	F						R	R
Administer OCSP Responders	F		F				R	R
Administer Support Servers	F		F				R	R
Administer OCSP Repeaters	F		F				R	R
Manage CAC PIN Reset Workstations	F		F				R	R

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
Administer leaf objects at PoR level	F						R	R
Administer group policy objects at PoR level	F	R	R	R	R	M	R	R
Administer group policy links and link order at PoR level	F	R	R	R	R	M	R	R
Remedy								
Remedy Admin - add users, manage workflow etc.	F	R					R	R
Administer Remedy servers	F	R					R	R
Remote Desktop Services								
Administer enterprise licensing servers	F						R	R
Administer enterprise RDS session hosts	F						R	R
Administer enterprise RDS environment	F						R	R
Administer enterprise RDS GPO settings	F						R	R
Administer command licensing servers		F	M				R	R
Administer command RDS session hosts		F	M				R	R
Administer command RDS environment		F	M				R	R
Administer command RDS GPO settings	F	R					R	R
Reverse Proxy								
Administer Web Application Proxy servers	F	R	R				R	R
Administer Web Application Proxy configuration	F	R	M				R	R
Session Border Controllers								
Administer Session Border Controllers	F	R	R				R	R
System Center Configuration Manager								
Administer SCCM servers	F						R	R
Administer SCCM permissions	F						R	R
Administer SCCM client settings	F	R	R	R	R	R	R	R
Administer SCCM collections at Net Bn/Act level	F	M	R				R	R
Administer SCCM collections at the Tactical Extension Level	F	R	M				R	R
Administer SCCM collections at BPS level	F	*	M	M			R	R
Administer SCCM roles	F	R	R	R	R	R	R	R
Administer Microsoft Update groups (WSUS)	F	R	M	R	R	R	R	R
Administer Electronic Software Delivery configurations	F	R	*	R	R	R	R	R

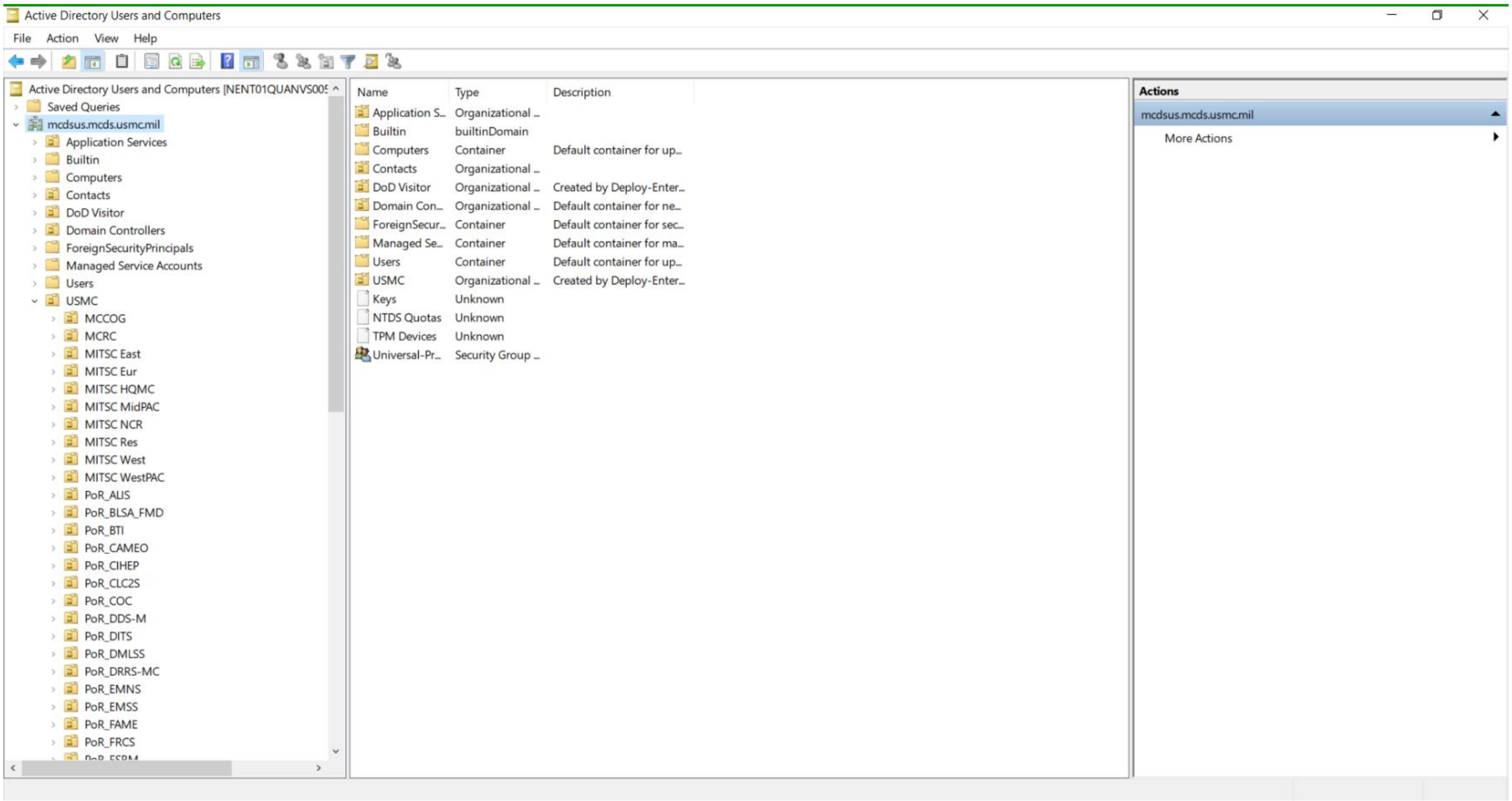
F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
Administer Operating System Deployment configurations	F	R	*	R	R	R	R	R
Administer and deploy configuration baselines	F	R	*	R	R	R	R	R
Administer and deploy Windows Defender settings	F	R	*	R	R	R	R	R
Administer and run reports within SSRS	F	R	*	R	R	R	R	R
Administer and run queries	F	R	*	R	R	R	R	R
Administer and run status messages	F	R	*	R	R	R	R	R
System Center Operations Manager								
Administer SCOM servers	F						R	R
Administer SCOM application	F						R	R
Administer SCOM portal	F						R	R
Generate reports	R	R	R	R	R	R	R	R
Administer custom reports	F	M	M	R	R	R	R	R
Administer management packs	F	R	R	R	R	R	R	R
System Center Orchestrator (Also See Azure Automation)								
Administer SCORCH servers	F						R	R
Administer SCORCH application	F	R	R				R	R
Administer automation tasks	F	M	M				R	R
System Center Service Manager								
Administer SCSM servers	F						R	R
Administer SCSM application	F						R	R
Administer SCSM portal	F						R	R
Run automation tasks	F		R				R	R
Generate reports	F	M	M	R	R	R	R	R
Administer custom reports	F	M	M	R	R	R	R	R
Server Builds								
Create or modify SHB	F						R	R
Create or modify VM templates from USMC SHB	F						R	R
Deploy VMs from template	F		M				R	R
Use USMC SHB to deploy physical servers	R	R	M	R	R	R	R	R
Create or modify SCCM OSD task sequences for server	F	R	R	R	R	R	R	R
Deploy SCCM OSD task sequences	F	R	R	R	R	R	R	R

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
Deploy VMs to non-Enterprise Equipment	F	F	F			F	R	R
Security Information and Event Management (SIEM)								
Administer, manage, and maintain MCEN SIEM infrastructure	F						R	R
Create and maintain SIEM accounts	F						R	R
Create and maintain SIEM policies	F						R	R
Access SIEM dashboard	F	R	R	R	R	R	R	R
Create and administer custom views	F	R	R	R			R	R
Create alarms	F	M	M	R			R	R
Patch and update SIEM servers	F						R	R
SQL								
Administer enterprise SQL servers	F						R	R
Administer enterprise-provided SQL databases	F	R	R				R	R
Storage								
Administration of Command Share at Net Bn/Act Level	F	F					R	R
Administration of Command Share at Tactical Extension Level	F		F				R	R
Administration of Command Share at B/P/S Level	F			F			R	R
Administration of Command Share at the TS/C Level	F		F		F		R	R
Administration of Command Share at the PoR Level	F		F			F	R	R
Administration of enterprise storage	F						R	R
Tanium								
Administer Tanium Servers and Services	F						W	R
Patch and Update Tanium servers and application	F						W	R
Access Tanium Console	F	R	R				W	R
Utility								
Administer utility servers	F							R
Administer source script / RDS licensing servers	F	R	R	R	R	R	R	R
Administer roles and features on utility servers	F	R	R	R	R	R	R	R
Administer applications on utility servers	F	R	R	R	R	R	R	R
Administer IPSec settings on utility servers	F							R

F=Full Control M=Modify (Add, remove, change) W=Write (Add, remove) R=Read (Read, audit) *=Inherited permissions blank=No access	MCCOG	Net Bn/Act	FMF	Base/Post/Station	Tenant/Supported Command	Program of Record	DCO Forces	IC4 White Team
Virtual Desktop Infrastructure								
Administer root domain controllers	F	R		R	R	R	R	R
Administer child domain controllers	F	R		R	R	R	R	R
Administer organizational units	F	R		R	R	R	R	R
Administer leaf objects at Net Bn/Act level	*	F		R	R	R	R	R
Administer leaf objects at Tactical Extension level	*		F				R	R
Administer leaf objects at B/P/S level	F	R		R	R	R	R	R
Administer leaf objects at T/SC level	F	R		R	R	R	R	R
Administer leaf objects at PoR level	F	R		R	R	R	R	R
Administer group policy objects	F	R		R	R	R	R	R
Administer group policy links and link order	F	R		R	R	R	R	R
Administer forest FSMO roles	F	R		R	R	R	R	R
Administer domain FSMO roles	F	R		R	R	R	R	R
Administer AD Integrated DNS Zones	F							
Administer service accounts	F	R		R	R	R	R	R
Administer AD Physical Components	F	R		R	R	R	R	R
Administer AD Schema	F	R		R	R	R	R	R
Administer forest and domain trusts	F	R		R	R	R	R	R
Administer USMC Enterprise Servers leaf objects	F	R		R	R	R	R	R
Administer USMC Enterprise Administration leaf objects	F	R		R	R	R	R	R
Patch and update domain controllers	F	R		R	R	R	R	R
Virtual Infrastructure								
Administer virtual servers at Net Bn/Act Level	F	W					R	R
Administer virtual servers at Tactical Extension Level	F		W				R	R
Administer virtual servers at B/P/S Level	F			W			R	R
Administer virtual servers at the TS/C Level	F				W		R	R
Administer virtual servers at the PoR Level	F		F			W	R	R
Administer enterprise virtual infrastructure	F						R	R
Chat								
Administer Cisco Jabber	F		F				R	R
Other Chat Applications (ie Transverse, MAKO etc)	F		F				R	R

Appendix B. MCEN Active Directory OU Structure

This Appendix provides a screenshot of the logical OU structure of MCDSUS AD domain. It does not contain all the OUs that exist in real time. The current AD structure can be viewed using the Active Directory Users and Computers application. MITSCs will be deprecated with the Network Battalions/Activities standing up.



- Active Directory Users and Computers [NENT01QUANVS005
  - Saved Queries
  - mcdsus.mcds.usmc.mil
    - Application Services
    - Builtin
    - Computers
    - Contacts
    - DoD Visitor
    - Domain Controllers
    - ForeignSecurityPrincipals
    - Managed Service Accounts
    - Users
    - USMC
      - MCCOG
      - MCRC
      - MITSC East
      - MITSC Eur
      - MITSC HQMC
      - MITSC MidPAC
      - MITSC NCR
      - MITSC Res
      - MITSC West
      - MITSC WestPAC
      - PoR_ALIS
      - PoR_BLSA_FMD
      - PoR_BTI
      - PoR_CAMEO
      - PoR_CIHEP
      - PoR_CLC2S
      - PoR_COC
      - PoR_DDS-M
      - PoR_DITS
      - PoR_DMLSS
      - PoR_DRRS-MC
      - PoR_EMNS
      - PoR_EMSS
      - PoR_FAME
      - PoR_FRCS
      - PoR_FSRM

Name	Type	Description
Application S...	Organizational ...	
Builtin	builtinDomain	
Computers	Container	Default container for up...
Contacts	Organizational ...	
DoD Visitor	Organizational ...	Created by Deploy-Enter...
Domain Con...	Organizational ...	Default container for ne...
ForeignSecur...	Container	Default container for sec...
Managed Se...	Container	Default container for ma...
Users	Container	Default container for up...
USMC	Organizational ...	Created by Deploy-Enter...
Keys	Unknown	
NTDS Quotas	Unknown	
TPM Devices	Unknown	
Universal-Pr...	Security Group ...	

Appendix C. References

A. Deployable MCEN Concept of Employment version 2.2.0 dtd 14 Nov 2017

B. MCEN Tactical Processing Node (TPN) Implementation Guide, Version 0.3 dated 17 Oct 18

C. Enterprise Cybersecurity Manual 007: Resource Access Guide Version 3.0

D. Enterprise Cybersecurity Manual 020: Marine Corps Information Assurance Vulnerability Management Program Version 1.0 dtd 31 Dec 2013

E. General Records Schedule 6.1: Email Managed under a Capstone Approach, Transmittal No. 26 dtd Sept 2016

F. Enterprise Cybersecurity Manual 019: Program of Record Cybersecurity Playbook Version 1.0 dtd 19 Apr 2019

G. IRM 2300-14: Enterprise Information Technology Service Management Identity and Access Management Process Guide

H. Marine Corps Bulletin 3100: Operations and Defense of the Marine Corps Enterprise Network dtd 14 Jul 2017

I. Marine Corps Enterprise Secret Internet Protocol Router Network Concept of Employment, Version 4.3 dtd 05 Apr 2010

J. Marine Corps Order 5239.2B: Marine Corps Cybersecurity dtd 05 Nov 2015

K. Marine Corps Strategy for Assured Command and Control dtd March 2017

L. MCEN Naming Standard for Application and Systems, Version 2.5 dtd 20 Feb 2018

M. MCEN Service Catalog: https://eris.mceits.usmc.mil/arsys/forms/ars/SRS%3AServiceRequestConsole

N. MCEN-N Jump Server Installation, D403.MCEN-N SYSLOG Server Installation, Version 1.0 dtd 14 Apr 2016

O. Request Fulfillment Standard Operating Procedures, MCCOG SOP D03-558 dtd 30 May 2017

P. Utility Server Design, D401. 253-20140501, Version 1.0 dtd 17 Nov 2016

Q. Marine Corps Order 3100.4a Cyberspace Operations

R. MCEN C2 MROC Decision Memorandum

S. ECSM 018 Marine Corps Assessment and Authorization Process (MCAAP) 04 June 2020

T. MCO 5239.2B Marine Corps Cybersecurity 05Nov2015

U. ECSM 018 Marine Corps Assessment and Authorization Process (MCAAP) 04 June 2020

V. MCO 5239.2B Marine Corps Cybersecurity 05 November 2015

W. ECSM 007 MEMO dated 15 November 2021 (Extension Attribute 12)