# SCCM Standards and Guidelines

**Effective Date:** 8/28/18  
**Document Owner:** Dilek Mascolo

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Revision Notes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>8/28/18</td>
<td>Dilek Mascolo</td>
<td></td>
</tr>
</tbody>
</table>

**Related/Referenced Documents:**
# Table of Contents

1. General Overview ......................................................................................................................................................... 3
2. Service Description .......................................................................................................................................................... 3
   2.1  Service Scope .......................................................................................................................................................... 3
   2.1.1  Area Unit Requirements to Use the Service ........................................................................................................... 3
   2.1.2  Boundaries of Service Features and Functions .................................................................................................... 4
   2.2  Service Level Performance ........................................................................................................................................ 4
   2.2.1  General Service Levels .......................................................................................................................................... 4
   2.2.2  Specific Service Levels .......................................................................................................................................... 4
3. Roles and Responsibilities .................................................................................................................................................. 4
   3.1  UNM IT Responsibilities in Support of the Service ..................................................................................................... 4
   3.2  Area Unit Responsibilities in Support of the Service ................................................................................................ 5
4. Hours of Coverage and Escalation ................................................................................................................................. 6
   4.1  Hours of Coverage .................................................................................................................................................... 6
   4.2  Service Exceptions to Coverage ................................................................................................................................ 6
   4.3  Escalation ................................................................................................................................................................ 6
5. Service Requests ............................................................................................................................................................... 6
   5.1  Service Request Submission ......................................................................................................................................... 6
   5.2  Service Request Response ........................................................................................................................................ 7
6. Incidents ............................................................................................................................................................................. 7
   6.1  Incident Report ............................................................................................................................................................ 7
   6.2  Incident Response ........................................................................................................................................................ 7
   6.3  Prioritization ............................................................................................................................................................... 7
7. Maintenance and Service Changes ................................................................................................................................. 7
1 General Overview

System Center Configuration Manager (hereon referred to as SCCM) is an infrastructure that provides colleges and departments the ability to manage and maintain their desktops and servers. Deploying and managing Windows is easier than ever before with new improvements including the support of the latest Windows 10 features, Windows in-place upgrade, more frequent and easier updates, unified end-user portal.

SCCM is available to Unit IT Administrators with an existing OU in UNM Active Directory - colleges.ad.unm.edu. SCCM follows a distributed support model similar to the UNM AD OU Administrator model where Unit IT Administrators are delegated full control of their Unit AD OU to perform SCCM tasks.

2 Service Description

UNM IT documents services in the UNM IT service catalog, http://it.unm.edu/servicecatalog/asset_list.php?type=2&a_id=109&a_recid=9400aa519d697cc57acc7d4bf29e83ba6b6ef507c8&dept=229&origin=az

2.1 Service Scope

Colleges and departments using the SCCM infrastructure will retain full control of their resources in their organizational units (OU) in addition to gaining the following benefits and fully supported features:

- SCCM access (roles/permissions) scoped to the unit’s AD OU structure
- Access to the SCCM console
- 2 baseline collections: All users and all devices in the unit’s AD OU(s)
- Ability to define custom collections of users and devices based on the 2 baseline collections
- Baseline (default) client settings for all enrolled devices in unit’s OU(s)
- Ability to define custom client settings to meet unit needs and apply to devices in unit’s AD OU(s)
- Windows operating system deployment (SOE standard operating environment – thin image via standard Task Sequence) to devices in unit’s AD OU(s)
  - In addition to SOE, unit administrators can also copy and then customize task sequence actions to suit their individual needs (Please see End User Responsibility section of this document)
- Access to driver packages for Dell hardware (5 years of previously supported standard hardware and the current hardware standard, found in the UNM IT service catalog)
- Deploy centrally managed applications (SOE applications and packages) to devices in unit’s AD OU(s)
- Create and deploy custom (unit specific) applications and packages to devices in unit’s AD OU(s)
- Execute centrally managed scripts against devices in unit’s AD OU(s)
- Create and deploy custom scripts against devices in unit’s AD OU(s)
- Adding new objects under ‘UNM shared security scope’ requires review and approval by the SCCM admin group (Please see Area Unit Responsibility section of this document)
- View hardware and software inventory for enrolled clients in unit’s AD OU(s)
- Use centrally managed reports and queries against devices in unit’s AD OU(s)
- Create custom (unit specific) queries against devices in unit’s AD OU(s)

Access to SCCM features not explicitly defined above may also be available (by default or by request) but full support for such features through UNM IT is not available.
2.1.1 Area Unit Requirements to Use the Service

- Complete SCCM training and OU Admin training
- View IT Alerts for scheduled maintenance and outages
- Network file share with sufficient storage to hold the custom images, applications and packages the department plans to deploy using SCCM; additionally, the AD group "SCCM-Distribution Point Servers-GG" must be granted read access to the share (both share and NTFS permissions)
- If a department intends to deploy images greater than 5 GB to more than 1 device at a time, the department must provide a Distribution Point in the subnets their devices reside in.
- If a department intends to deploy packages or applications greater than 1 GB in size, the department must provide a Distribution Point in the subnets their devices reside in. Limited bandwidth sites may also require a Distribution Point.
- Distribution Points (hardware and software) must meet the following requirements see FI #7739

2.1.2 Boundaries of Service Features and Functions

- Area Units will only use UNM owned infrastructure and equipment;
- Area Unit will make a reasonable effort to determine where the problem lies, prior to contacting UNM IT;
- IT will retain administrative access to SCCM and associated components like Distribution Points;
- Services hosted by IT are being provided to Area Units only. Any resale of this service must be disclosed in advance, in writing to the Service Owner;

2.2 Service Level Performance

2.2.1 General Service Levels

- Response to reported incidents and service requests as defined in Sections 5 and 6 below;
- Customized SCCM training;

2.2.2 Specific Service Levels

- Monitoring system with alerts;
  - Alert will be sent to UNM IT Platforms administrators if the UNM Shared DP capacity reaches 90%
  - Alert will be sent to UNM IT Platforms administrators if the SCCM infrastructure is under a sustained, heavy load (slow performance.)
  - Alert will be sent to UNM IT Platforms administrators if the SCCM infrastructure is inaccessible;

3 Roles and Responsibilities

3.1 UNM IT Responsibilities in Support of the Service

UNM IT responsibilities and/or requirements in support of these standards and guidelines include:

- Periodic (semiannual) review and update of SOE (Standard Operating Environment) components, including Windows images, Boot images, Applications and Packages;
- Standardized onboarding process such that each onboarded unit receives:
  - Permissioned folders for custom items under Device Collections, User Collections, Applications, Packages, Queries, Task Sequences, and Operating System Images
  - 2 baseline collections, scoped to the unit’s AD OU: All <OU> Users (AD query against the unit’s Users OU) and All <OU> Computers (AD query against the unit’s Workstations OU)
SCCM user with the following Security Roles (privileges), mapped to the unit’s AD OU Admins group:

- UNM – Reporting User
- UNM – Import Computer
- UNM - Deploy Shared Applications
- UNM - Operations Administrator

- Unit specific Security Scope, applied to the unit’s baseline collections and administrative user
- Global Security Scopes (Default and UNM – Shared Items) that allow use of Reports and privileges to be executed against shared items

- Providing and maintaining reusable GPOs that can be leveraged by units to apply the required SCCM settings to devices in their OUs;
- Providing a shared Distribution Point with reasonable (approximately 5 GB) capacity for units whose SCCM usage does not warrant a local Distribution Point;
- Facilitating periodic SCCM Administrators Committee meetings to discuss application/package sharing, common questions, and issues;
- Maintaining proper security scope on centrally managed (SOE) items, including Boot Images, Images, Applications, Packages, Drivers and Driver Packages;
- Ensuring consistent distribution of centrally managed (SOE) items, including Boot Images, Images, Applications, Packages, Drivers and Driver Packages;
- Maintaining default Client Settings;
- Maintaining global SCCM security roles;
- Maintaining the SCCM infrastructure such that all component versions are supported by Microsoft;
- Coordinating and assisting unit’s with the setup and deployment of distribution points;
- System operations, administration and network connections;
- Web access to include service catalog, billing portal, self-service portal;
- System level backup processes and disaster recovery (does not include DPs);
- Basic up/down system monitoring;
- Friendly, courteous and efficient service;
- Support services via UNM IT Service Desk;
- Prompt referral of any inquiries/complaints to the appropriate responsible team;
- Continuous effort to develop and improve services for all service users.
- Meet response times associated with the priority assigned to incidents and Service Requests;
- Generate reports on service level performance;
- Adhere to established Maintenance windows;
- Publish all scheduled maintenance and service updates via:
  - IT Alerts at https://italerts.unm.edu;
  - IT-SCCM-L email;

### 3.2 Area Unit Responsibilities in Support of the Service

Area Unit responsibilities and/or requirements in support of these standards and guidelines include:

- Adhering to UNM’s SCCM naming standards (every item created in SCCM must be named starting with the owning unit’s OU name and a “-”. Example: <OU> - <Description of item> or IT – All Manager Workstations)
- Ensuring the SCCM client is installed and properly configured on all unit devices managed through SCCM;
- Maintaining proper security scope on custom items, including Boot Images, Images, Application, Packages, Drivers and Driver Packages
• Ensuring physical and network security of DP;
• Ensuring compliance with licensing agreements (and license availability) when deploying custom operating systems, applications and packages;
• Completing SCCM onboarding training and OU Admin training; complete additional/ongoing training (provided by a 3rd party) as needed to support the usage of SCCM within the unit;
• Understanding and complying with standards surrounding custom Client Settings (Not changing: client polling interval, compliance polling interval, cloud services, maximum custom MIF file size, wake-up proxy, state message reporting cycle,
• Understanding and complying with standards surrounding Collection updates, including: Never enabling “Incremental Updates” and understanding that “Full Update” timing is programatically set to a random time between 12:00 AM and 7:00 AM daily;
• Monitoring IT Alerts and the IT-SCCM-L email list for service notifications and updates;
• Consider any policy implications or responsibilities;
• IT Strategic Advisory Committee to collaborate with UNM IT on the service framework to satisfy the University of New Mexico business requirements.
• Contact UNM IT Service Owner for additions or changes in established service levels;
• Comply with UNM Business Policies 2500, 2520, 7215.
http://policy.unm.edu/university-policies/2000/2500.html
http://policy.unm.edu/university-policies/2000/2520.html
https://policy.unm.edu/university-policies/7000/7215.html

4 Hours of Coverage and Escalation

4.1 Hours of Coverage
SCCM service is provided 24 hours a day 7 days a week except for periods of planned maintenance.

4.2 Service Exceptions to Coverage
Describe any exceptions or This section intentionally left blank.

4.3 Escalation
If you are not satisfied with the level of service on a request, please contact the Service Owner and if necessary, the UNM IT Service Manager.

<table>
<thead>
<tr>
<th>UNM IT Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Service Owner</td>
</tr>
<tr>
<td>Service Manager</td>
</tr>
<tr>
<td>Subject Matter Expert (SME)</td>
</tr>
</tbody>
</table>

5 Service Requests
A Service Request is defined as a request for information, advice, or for access to a service.

5.1 Service Request Submission
Service Requests can be submitted by calling 505.277.5757. Current hours of operation are listed on the Customer Support Services website, http://it.unm.edu/support.

Online Service Requests can be submitted at the following URL: https://help.unm.edu.
5.2 Service Request Response
For all requests, UNM IT’s objective is to acknowledge and assign requests within twelve (12) business hours of receipt. Requests will be fulfilled within seven (7) days.

Campus priorities may require exceptions during certain times of the Academic year.

6 Incidents
An incident is defined as any interruption in the normal functioning of a service or system.

6.1 Incident Report
Incidents can be reported using Help.UNM at https://help.unm.edu or by calling the UNM IT Service Desk during business hours at 505.277.5757.

For service outages after hours, call 505.277.5757 and select Option #3 to leave a message for the Manager on Duty (MOD). The MOD will contact the appropriate service technician to help resolve the service outage.

6.2 Incident Response
Response time objectives for incidents reported to UNM IT are as follows:
Priority 1 (P1) is acknowledged, accepted and resolved within four (4) clock hours.
Priority 2 (P2) is acknowledged, accepted and resolved within one (1) business day.
Priority 3 (P3) is acknowledged, accepted and resolved within four (4) business days.
Priority 4 (P4) is acknowledged, accepted and resolved within nine (9) business days.

6.3 Prioritization
All reported incidents receive a priority number based on the impact and urgency of the service interruption.

Impact is determined based on the number of people/Departments/buildings that are affected by the interruption or outage. Life-Safety issues are taken into consideration for assessing and assigning priorities.

Urgency is based on the acceptable delay to restore the service. Urgency can be critical or high and is determined based on the nature of the service outage.

UNM IT may prioritize incoming incident requests as P1 or P2 priority if it meets one or more of the following criteria:

- Significant number of people affected;
- The level to which work is impaired for individuals;
- Academic and Administrative Calendar deadlines;
- Significant impact on the delivery of instruction;
- Significant risk to safety, law, rule, or policy compliance.

7 Maintenance and Service Changes
The Maintenance Window for SCCM can be found on the UNM IT website, http://it.unm.edu/availability under the “All Services” category.

UNM IT reserves the right to modify the maintenance window.