LA-UR-14-26943
Approved for public release; distribution is unlimited.

Title: OCMIS User Guide

Author(s): Bingman, James Boyd Dustin

Intended for: Report

Issued: 2014-09-04

OCMIS User Guide

Site Overview

The Operational Continuous Monitoring (OCMIS) web portal is a simple yet effective method of displaying the necessary information of continuous monitoring of operations within LANL networks. Such information includes audit log metrics, dates and times of audits, user information including approval, renewal and removal process, incidents, and hardware and software inventories. OCMIS is designed with transparency of operations in mind and strives to make data and information easy to access and simple to understand. The site will also allow for the simple addition of information and requests for network accounts and software from one location.

Continuous Monitoring

The main purpose of the site is to assure that continuous monitoring of network assets is being provided in a transparent way to DOE. There are two types of continuous monitoring. The first type is Technical continuous monitoring. This form of monitoring takes place on the back end of individual information systems using CPAT information along with AUReport for Linux environments and Elm for Windows environments to produce metrics data. The 11 domains of continuous monitoring guide required data.

The 11 Domains Of Continuous Monitoring are as follows:

1 - Vulnerability Management: CPAT information relating to False/Positives and Deviations (graphs showing monthly data)

2 - Patch Management: Evidence Showing when systems where patched

3 - Event Management: Statistics on Log information (Graph showing trends)

4 - Incident Management: Provide number of incidents and explanations where appropriate (Graph showing data over 1 year)

5 - Malware Detection: When malware was detected, severity level and how it affects risk (Risk analysis with pie chart)

6 - Asset Management: Hardware replacement trends for security significant items (Trend Analysis)

7 - Configuration Management: Transparency for # of users both privileged and non-privileged

8 - Network Management: Evidence and tracking of PTS/Tempest Inspection dates

9 - License Management: Listing of All software including 3rd Party applications (Tracking approvals and changes)

10 - Information Management: Training statistics

11 - Software Assurance: Tracking and providing metrics on version updates and how it affects risk

Data Call Information

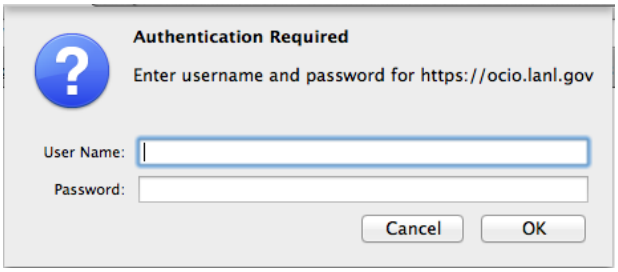
Gathering of Data Call information will be one of the uses of OCMIS. In the PAD GS ISSP page on OCMIS, all 11 Domains of Continuous Monitoring are listed on the left. Each domain that is listed has its own sub-section that meets the metrics display requirements of that domain.

To gather information of the number of privileged and non-privileged users of networks follow the steps below:

Step1. Access OCMIS

a. Open a web browser and type ocmis.lanl.gov

b. Login with Z# and WIN Password



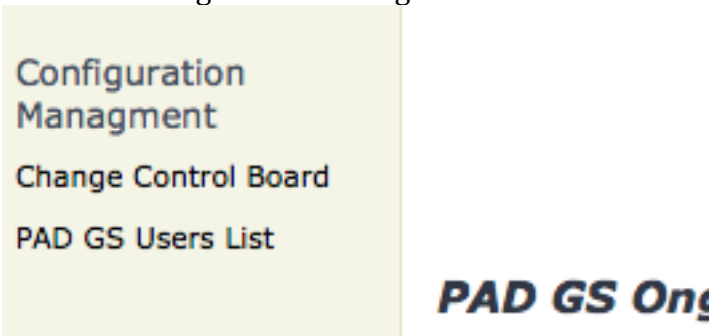
Step2. Select network

Networks appear on the quick launch bar on the far left.

a. Click PAD GS

Step3. Click PAD GS Users List

This can be found under Configuration Management



Here one can easily view the number of privileged and non-privileged users that are approved to access the PAD GS network.

To look up information of the number of systems on a network, the system types, their owners, or any other data about systems on the network follow the steps below:

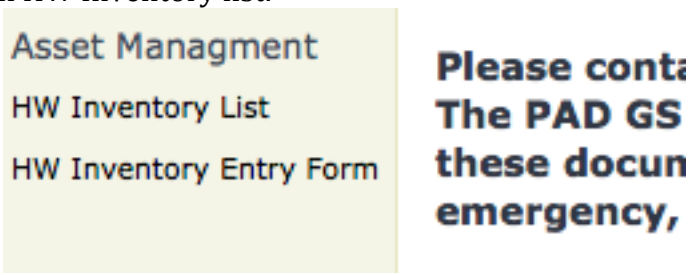
Step1. Access OCMIS

a. Open a web browser and type ocmis.lanl.gov
b. Login with Z# and WIN Password.

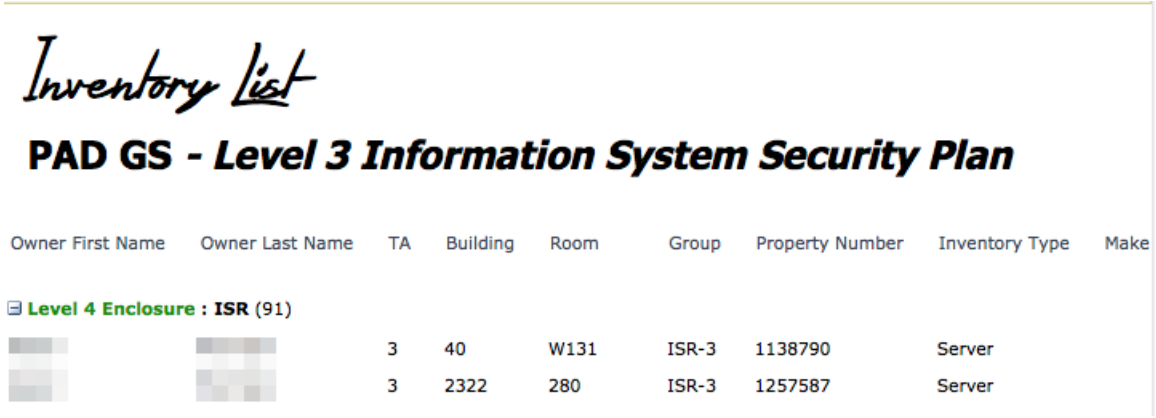
Step2. Click PAD GS

Step3. Go to HW Inventory List under Asset management

a. Click on HW Inventory list.



b. Click on the plus icon next to the level 4 Enclosure that needs to be documented.



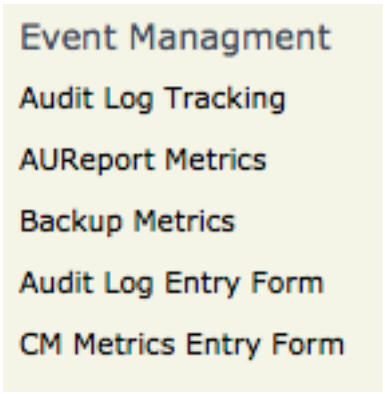
This page will show one all of the previously mentioned data as well as the equipment's location and property number.

Continuous Monitoring and Metrics Data

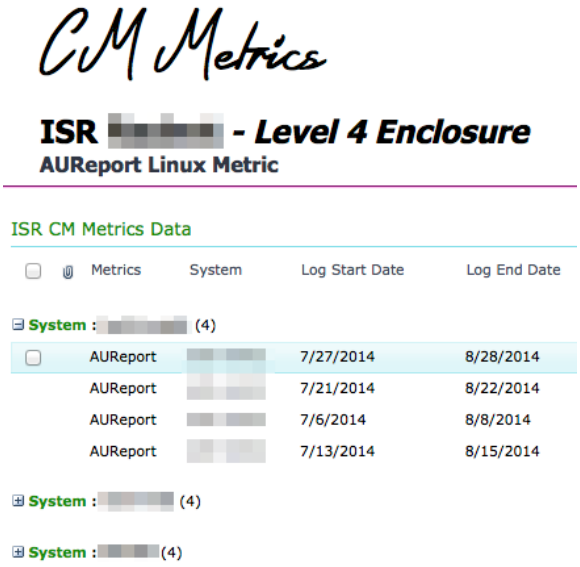
System metrics data can also be viewed to determine ominous changes in patterns over time. Such system changes can be viewed under Event Management in AUReport Metrics.
To access AUReport Metrics:

Step1. Access OCMIS
- a. Open a web browser and type ocmis.lanl.gov
- b. Login with Z# and WIN Password

Step2. Click on PAD GS
Step3. Under Event Management, click AUReport Metrics



Step4. Click the plus sign by the desired system



Here, The raw metrics data can be viewed along with graphical representations of that data.

Managed by The ISSO

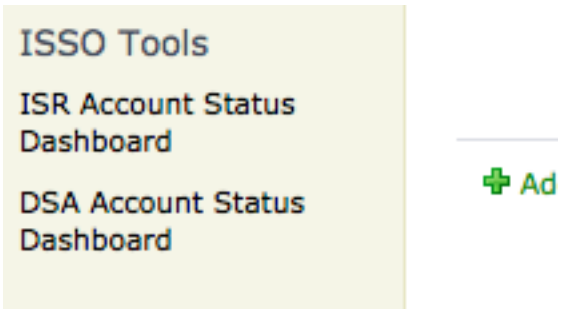
The ISSO of each network will manage his/her own sites and pages. There duties include managing user status on the Account Status Dashboards, entering metrics data, and modifying information as needed in the data sheet views of data lists.

The ISSO can access the dashboards by following these steps:

Step1. Access OCMIS
- a. Open a web browser and type ocmis.lanl.gov
- b. Login with Z# and WIN Password

Step2. Click on PAD GS

Step3. Under ISSO Tools, click ISR Account Status Dashboard



Here, the ISSO can view user workflow items and their status. These workflows include network account requests, network account renewals, and network account disabling. This allows the ISSO to monitor the status of workflows and training involved with network access.

Other areas that require the use of the ISSO are the data entry forms. These forms are needed, as metrics cannot currently be automatically transferred from the scanning systems directly to the lists on the OCMIS site.

The ISSO can access the Audit Log, CM Metrics, or Network Inspection entry forms by following these steps:

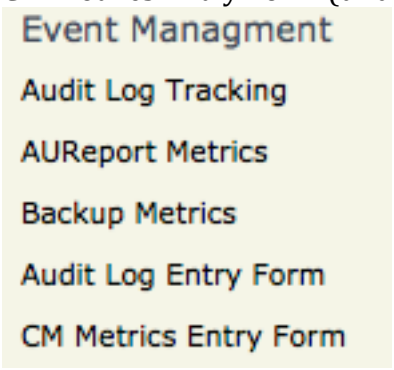
Step1. Access OCMIS
- a. Open a web browser and type ocmis.lanl.gov
- b. Login with Z# and WIN Password

Step2. Click on PAD GS

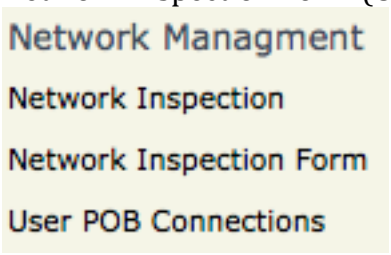
Step3. Click on an entry form

I. Audit Log Entry Form (under Event Management)

II. CM Metrics Entry Form (under Event Management)



III. Network Inspection Form (Under Network Management)

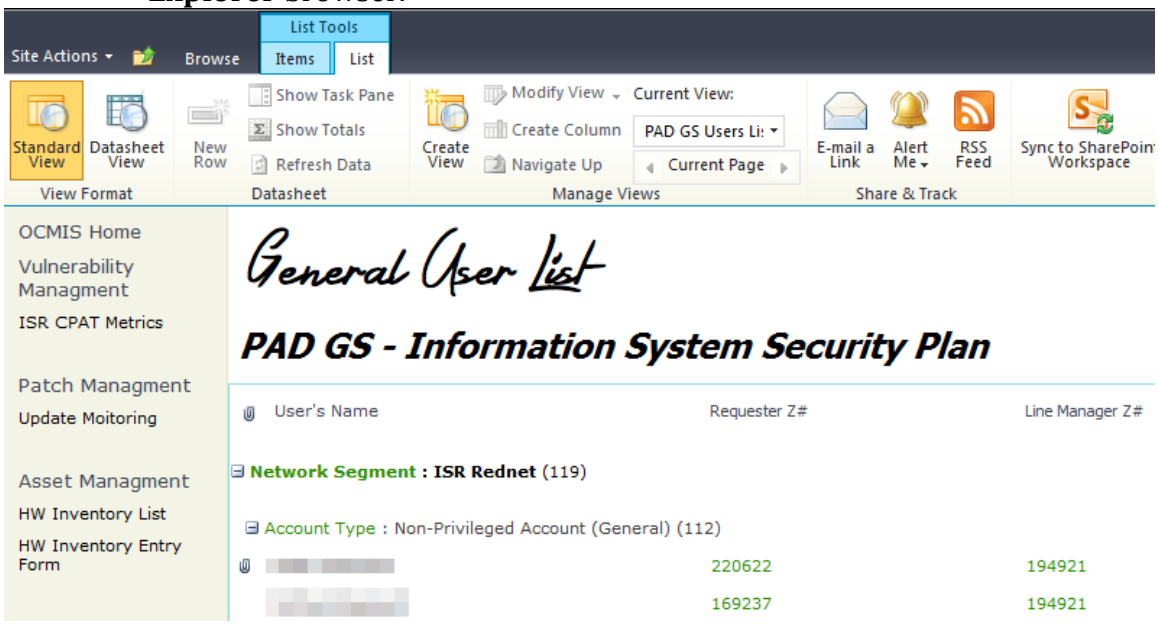


Each of these forms contains not only simple data entry boxes, but also drop down lists that allow for the filtering and organization of data for quick and easy reference.

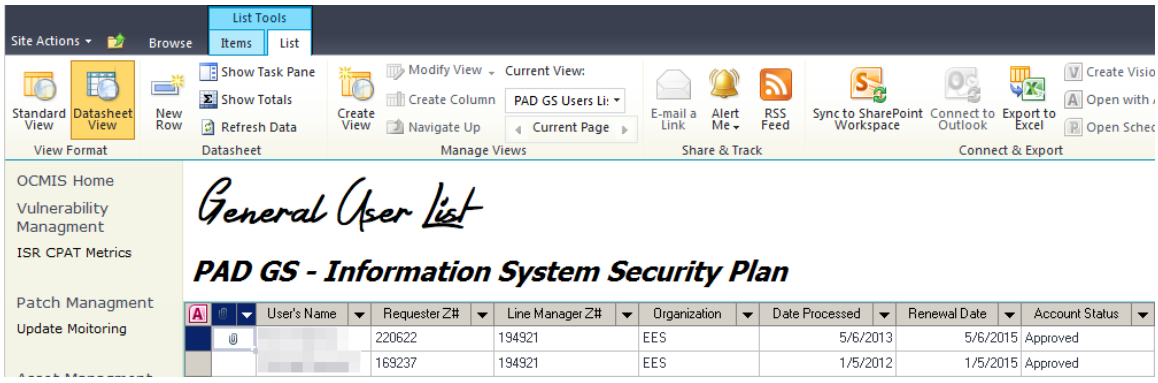
The ISSO will also utilize the data sheet view of each list when necessary for data correction and manipulation. This method of data entry and manipulation easily allows the ISSO to import data from old Excel or Access files via copy and paste. The ISSO can access the data sheet view by first accessing one of the pages that has a previously generated list and then following these steps.

Step1. Click inside the list

Step2. Click List under List Tools in the upper left corner of the **Internet Explorer** browser.



Step3. Click Datasheet View in the upper left corner of the **Internet Explorer** browser



User Requests

Users will also be able to use the site to expedite the process of getting the network access that is needed to achieve mission objectives. A user can request access to a mission necessary network by following these steps.

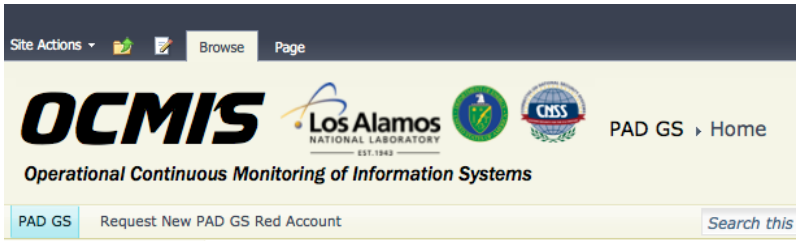
Step1. Access OCMIS

a. Open a web browser and type ocmis.lanl.gov

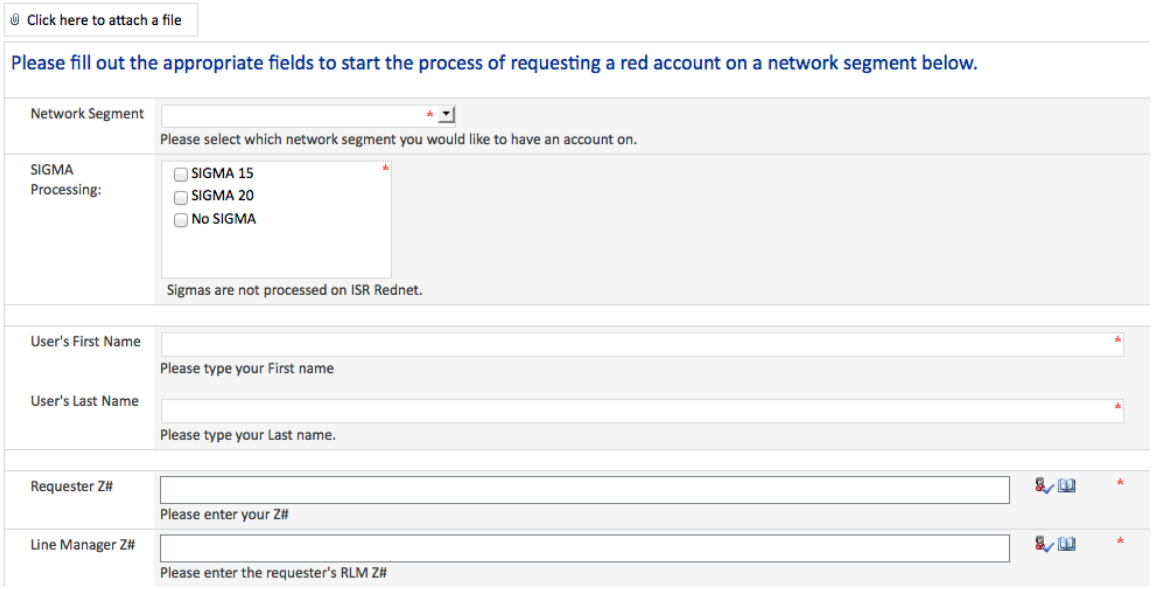
b. Login with Z# and WIN Password

Step2. Click on PAD GS

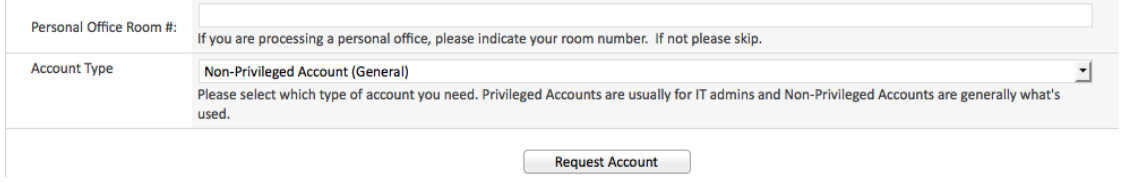
Step3. Click on Request New PAD GS Red Account in the upper left corner of the browser.



Step4. Fill out the form



Step5. Click Request Account



Once the form is filled out and submitted, a workflow that was designed for that form will start. The proper authorities are automatically emailed and notified about the request. These authorities have the authority to deny the request, or

approve it and send the request further up the chain. Signatures in this case are replaced by WIN credential login authentication for identity verification. Risk in this process is mitigated by having weekly meetings to review new accounts.

Workflows also track the data in the user lists that are generated allowing for automatic reminders of renewal dates. This notification of renewal dates, that are upcoming or past due, can be seen by the ISSO in the Account Status Dashboards. User's account status is constantly updated as the workflow automatically replaces account metadata as set variables within the workflow occur. This allows for automated tracking and documentation of users within the network.

Future

Sharepoint is a one-stop shop for data tracking, document archival, departmental/team collaboration, transparent communication and distribution of information, and automation of tedious tasks. One of those tedious tasks will be the entry of data metrics by the ISSO.

The implementation of data links is currently not active. However, when they are implemented, Technical Continuous Monitoring tools will be set up to automatically enter those metrics as soon as they are attained. This will allow a faster and more up-to-date window into the operations of the networks. This automatically generated information can also be used to form pre-formatted data call reports that can be viewed or downloaded on the fly.

Sharepoint is was chosen for all of the tasks mentioned previously, not only because it is fully capable of performing all of those tasks, but also because LANL has been using it for quite sometime already. The hardware and software infrastructure already exists in LANL along with the support staff to keep it running.

Sharepoint sites are quickly and easily built without need to get into the underlying code for a normal site to function. This allows for seemingly complex processes to be built and automated by an administrator with a cursory knowledge of Sharepoint. Because of this, little training is required to build and operate such a Sharepoint site. Noting the ease of building a Sharepoint site, the exporting of an existing Sharepoint site can be done easily with, or without, the underlying data allowing for site templates to be stored for easy replication within LANL.

Sharepoint is an excellent tool for transparency of information, task automation, and data storage and organization. The speed and ease of all of these operations result in a great time and cost savings by replacing and improving antiquated methods and processes.