

Creating MSOffice SharePoint service account managers without providing excessive control

By CW3 Eric Bray

Microsoft Office SharePoint Service provides an easy, web based platform for users to collaborate on the web, but efficient user management out of the box is lacking.

As an automations chief with only a handful of administrators - few with any MOSS training or experience - I cannot afford to give away unrestricted permissions to subordinate personnel simply to add users to our portal site. My unit has close to 7000 personnel in dispersed geographic locations throughout the world. It is inefficient to require system administrators to manage portal accounts all day as users relocate. If we allow subordinate personnel the right to add users, we risk creating more work for system administrators because of the need to maintain acceptable knowledge management practices. Poor KM discipline leads

to SharePoint sprawl with data spreading out in a disordered fashion.

Over the last 18 months, my team has been working with a new work flow server by K2 called BlackPearl. The BlackPearl server is a workflow application that can be installed as a standalone server, or on the backside of a Web front end. In our case, the software is installed on the back end of SharePoint. We are still using MOSS07 but plan to upgrade in the next year. Presently we have created several business Process Automations. However, the process we are covering in this article is known as "On boarding." Figure 1 below is a depiction of On boarding which allows non-systems administrators to manage and create accounts with the right permissions without losing control of the website and reducing overall Sprawl.

The requirements for this

workflow are twofold. First, on tactical platforms, we need to give new users the ability to request a new account with full access rights (Active Directory, Exchange, MOSS, and Adobe Connect or AC) to a non-classified Internet protocol router/secure Internet protocol router platform by way of a Web page. We are still testing this process and have achieved with great success even though a few bugs remain. Overall we have greatly reduced account creation and processing time on deployments. This request is auctioned, and accuracy is verified, by the knowledge management representative, but access is not granted until a review is completed by the system administration or help desk personnel. Secondly, on reach back systems, the workflow must also provide portal access to our subordinate users who are not in the same AD forest.

The current solution on



Figure 1. Onboarding



our NIPR reach back system (the latter) allows a KMR to go to a portal site, and authorize a user “registration access” rights in our portal. This is accomplished by way of audience based participation. Presently this process is on a separate site collection where the user can only see the acceptable use policy and request access by filling out the information required to establish a user account. No personal identifiable information is allowed. This information provides basic contact information and the fields necessary to complete a DA 2875 - System Authorization Request as a paperless process.

To better illustrate the workload, our chemical, biological, radiological, nuclear, and high yield explosives net portal has the root site (approximately 7 main groups), approximately 20 section sites (at least three groups per site); each section having anywhere from several to 10 sub-sites or “Shops” (at least 3 groups per shop also). At this time, we have about 300 SharePoint groups to manage on this server alone.

A visitor only gets read access to the root, section, and shop sites. The standard user gets root site (read), section (read/write), and shop level (read/write) access. The KMR (account / content

manager) has the same as a standard account, plus the ability to approve new users for read/write access to designated sites. The CBRNE net site is designed to filter information - usable and relevant information - into decision making material. Therefore, site design is maintained at the KM level and none of the users have the ability to change the site (in order to avoid “sprawl”). We will have internal sites later to enhance and enable creativity, but we just have not yet built that out.

CW3 Eric Bray began his military career as an MLRS fire direction specialist in Field Artillery in 1996. In 2000, he transitioned to Aviation as a Blackhawk pilot. He deployed in support of OIF three times. In 2008, he transitioned to Signal as a 254A. CW3 Bray is MSCA, MSCE, and Security Plus certified and is responsible for ensuring mission critical communications servers are up, secure and accessible to Soldiers of the 20th Support Command, subordinate units and inter-agency partners. He is the chief of automations, knowledge management for the 20th Support Command and is currently working business process automations via workflow servers. 

ACRONYM QuickScan

AC - Adobe Connect
AD - Active Directory
AKO - Army Knowledge Online
AUP - Acceptable Use Policy
BPA - Business Process Automation
CBRNE - Chemical, Biological, Radiological, Nuclear, and High Yield Explosives

KM - Knowledge Management
KMR - Knowledge Management Representative
MOSS - Microsoft Office SharePoint Service
NIPR - Non-classified Internet Protocol Router Network

PII - Personal Identifiable Information
SAAR - System Authorization Request
SIPR - Secure Internet Protocol Router Network
SysAdmin - System Administrator
WF - Windows Workflow Foundation