Dadeschools.net
Site Administrator Security Settings
Request for Comment (RFC)

This RFC was prepared by the Information Technology Services (ITS) Department of Miami-Dade County Public Schools (M-DCPS). Significant input was provided by school based technicians as well as other district technology groups through the M-DCPS Site Administrators Policy Committee. The RFC has undergone several draft revisions over the past two months based on input from members of the Site Administrators Policy Committee and the ITS Data Security Department.

All of the issues presented by the members of the committee and the ITS Data Security Department have been addressed and approved. ITS is now soliciting comments from the larger M-DCPS technical community. The ITS Data Security Department and the Site Administrators Policy Committee will meet in March of 2004 to discuss any comments that have been received and make any needed modifications to the RFC. It is anticipated that version 1.0 of the RFC will be finalized at that time and implemented as policy. Comments regarding this RFC should be sent to: bhofmann@dadeschools.net

Comment on this RFC will not stop once version 1.0 is implemented as policy. New versions may be developed, commented on and implemented in the future.

ITS would like to thank the following members if the Site Administrators Policy Committee for assisting ITS in the preparation of the initial RFC:

Hiram Duenas	Kenwood Elementary
David Huauya	Bilingual Education
Claudio Miranda	Instructional Technology
Oscar Morejon	John A. Ferguson Senior High
Robert Smith	Wesley Matthews Elementary (Currently with Network Services)

Overview

1. Purpose of the RFC

The dadeschools.net single domain model requires a delegation of some administrative tasks to school and other site administrators. The purpose of this document is to describe the permissions each site administrator will have and the tasks they will be able to carry out based on those permissions. This document will eventually become a standard for the school district and a serve to clarify the role of site administrators.

2. Site Administrators Policy Committee

A Site Administrators Policy committee prepared the initial RFC. The committee was composed of ITS staff, members of various technology related departments and school based site administrators. The purpose of the committee was to assist ITS with the technical details of the RFC and ensure that it met the following requirements:

A. The permissions and the tasks defined in the RFC are in alignment with the duties the site administrators are expected to perform
B. The permissions and tasks comply with the security needs of the school district

3. Establishment of Organizational Units

In order to meet the requirements above, three types of Organizational Units (OUs) will be established in the dadeschools.net domain for the use of site administrators. They are:

A. Site Based Security Groups - These OUs will enable the site administrators to establish security groups and control the membership of the groups within their OU. This will give site administrators the ability to control user access to resources within the site. The site administrator will not be able to create additional OUs within this OU or apply group policies to this OU.

B. Site Based Computer Accounts – These OUs will allow the site administrator to apply group policies to member servers and workstations in their site. This will enable the site administrator to limit the access of users on some workstations and improve security and control at the site. The site administrator will also be able to establish additional OUs within this OU.

C. Site Based User Accounts - These OUs will give the site administrator the ability to set up and administer local user accounts. Site based accounts are for users other than employees of M-DCPS. Some examples of site based accounts would be students, temporary workshop attendees, and software or hardware vendors. Site administrators will have control of the creation and administration of these user accounts. The site administrator will also be able to establish additional OUs within this OU and apply group policies to these OUs and to the OU as a whole.

4. **Establishment of Site Administrator Groups**

Each set of site OUs will be administered by an appropriate group of site administrators. Membership in each of each site administrator group will be determined by the ITS Data Security Department.

5. **Employee Accounts**

Employee accounts will be controlled by ITS. The creation and deletion of all employee accounts as well as all policies related to these accounts will be determined by the ITS Data Security Department. Site administrators will have the ability to execute only the following tasks on employee accounts at their site:

A. Reset passwords and unlock accounts
B. Require the user to change their password at next logon
C. Read and write the user's logon script path
D. Read and write the user's profile path
E. Read and write the user's home drive
F. Read and write the user's home folder

Technical Specifications

6. **Site Administrators Group –** Specifications and creation

The site administrators global security group will be created within the site OU within the District OU. This OU and global security group will be under the control of the ITS Data Security Department. The group name will be XXXXSiteAdmins where XXXX represents the location number of the site.

7. **Site Based User Accounts -** OU Configuration and Administration

An OU for each site will be created under the Site Based Accounts OU. The site based OU will be named XXXX where XXXX is the site location number. Delegation of Control is accomplished using the Delegation of Control Wizard and selecting the appropriate XXXXSiteAdmins group for the delegation. The following tasks will be delegated:

A. Create, delete, and manage user accounts
B. Reset user passwords and force password changes at next logon
C. Manage group policy links
D. Generate resultant set of policy (Logging)
E. Generate resultant set of policy (Planning)

After the OU is created using the wizard and the tasks delegated as above, bring up the properties of the OU. Click on the "Security" tab and then click on the "Advanced" button. In the "Advanced Security Settings" window, click on the "Add" button and select the XXXXSiteAdmins as the group to give additional permissions. In the "Permissions Entry" window click on the "Object" tab to give the

XXXXSiteAdmins permissions to make changes to specified objects within the OU. In the “Apply onto:” drop down list select “This object and all child objects”. Scroll down the permissions list box. Select:

A. Create Organizational Unit Objects
B. Delete Organizational Unit Objects

Click on OK and exit the security settings.

This Configuration will allow the site administrator to manage site based user accounts, apply group policies, and create additional OUs within this OU. Site administrator will be able to apply and test group policies. By default, site administrators will not be able to create group policies.

8. Site Based Security Groups - OU Configuration and Administration

An OU for each site will be created under the Site Based Groups OU. The site based OU will be named XXXX where XXXX is the site location number. Delegation of Control is accomplished using the Delegation of Control Wizard and selecting the appropriate XXXXSiteAdmins group for the delegation. The following tasks will be delegated:

A. Create, delete, and manage groups
B. Modify the membership of a group

This Configuration will allow the site administrator to manage site security groups. User accounts from anywhere in the domain can be give access to resources controlled by the site administrator. Site administrators will not be able to create OUs within this OU or link this OU to group policies. This is to ensure that site administrators do not apply group policies to employee accounts.

9. Site Based Computer Accounts - OU Configuration and Administration

An OU for each site will be created under the Site Based Computers OU. The site based OU will be named XXXX where XXXX is the site location number. Delegation of Control is accomplished using the Delegation of Control Wizard and selecting the appropriate XXXXSiteAdmins group for the delegation. The following tasks will be delegated:

A. Manage group policy links
B. Generate resultant set of policy (Logging)
C. Generate resultant set of policy (Planning)

After the OU is created and the tasks delegated as above, open the OU’s property window. Click on the “Security” tab and then click on the “Advanced” button. In the “Advanced Security Settings” window, click on the “Add” button and select the XXXXSiteAdmins as the group to give additional permissions. In the “Permissions Entry” window click on the “Object” tab to give the XXXXSiteAdmins permissions to make changes to certain objects within the OU.

In the “Apply onto:” drop down list select “This object and all child objects”. Scroll down the permissions list box and check off:

A. Create Computer Objects
B. Delete Computer Objects
C. Create Organizational Unit Objects
D. Delete Organizational Unit Objects

Click on OK and exit the OU properties window.

This Configuration will allow the site administrator to manage computer accounts at the site, create additional OUs, and apply group policies. Site administrators will be able to apply and test group policies. By default, site administrators will not be able to create group policies.

10. Employee Accounts – Delegation of Tasks to Site Administrators

Delegation of Control is accomplished using the Delegation of Control Wizard and selecting the appropriate XXXXSiteAdmins group for the delegation. The most efficient way to do this is to run the Delegation of Control Wizard twice. The first time, delegate only the following task to the site based administrator: Reset user passwords and force password change at next logon.

Run the Delegation Control Wizard a second time. The second time select “Create a custom task to delegate”. On the next screen select “Only the following objects in the folder”. Scroll to the bottom of the list and check “User Objects”. Leave the Create and Delete check boxes at the bottom of the screen unchecked. On the next screen, check the “General” and “Property Specific” check boxes. Scroll down the list and check the following boxes and complete the delegation process:

A. Read Home Drive
B. Write Home Drive
C. Read Home Folder
D. Write Home Folder
E. Read Profile Path
F. Write Profile Path
G. Read Script Path
H. Write Script Path
I. Read lockoutTime
J. Write lockoutTime

These delegations allow the site administrator to reset passwords for employee accounts at their site and unlock accounts that have been locked out. It also permits them to configure any of the options related to the user’s profile.