Current HFM Security

The security wrapped around HFM production is a combination of Network Security, DCOM Security and HFM Application security. The outer layer of security, Network Security, is comprised of domain registered groups. The middle layer of security, DCOM, integrates the outer and inner layers of security. HFM Security is the inner-layer of security that is defined by default and specific privileges associated to each group. Within HFM Security exists a Process Management feature that controls and follows the data through each step of the financial close process. Process Management uses data specific controls placed on the Scenario, Year, Period, Entity, and value dimension which control who can review, submit, promote, approve, reject or publish information. Phase One of implementation does not include HFM Process Management.

Network Security

Domain groups were created, with the hfm preface. Currently there are five groups, hfm_admin, hfm_fin, hfm_rptdev, hfm_journals, hfm_users. Their specific functions are detailed in the HFM Security section. These groups have the following attributes:

1. Control the login mapping that occurs every time a machine is rebooted.
2. All HFM users in the finance group (hfm_fin) are mapped to a share directory on mbia-amk-hfm02 called 'externalfiles' and share the common drive letter 'K' for clarity and consistency. Files in this directory consist of the application metadata outline, grid display files, rules for the application, and member list files.
3. All HFM users in the journals group (hfm_journals) are mapped to a share directory on mbia-amk-hfm02 called 'hfmuser' and share the common drive letter 'K' for clarity and consistency. Files in this directory consist primarily of data explorer grid templates and journal templates.
4. New HFM users are only added to the domain group, not the application; facilitating and centralizing the administration of HFM applications in the IT department. If someone's responsibilities change, he is moved to another group. If the individual leaves the company, the access to HFM is terminated as soon as the id is removed from Active Directory.

DCOM Security

Dcom security, Distributed Component Object Model, determines if a user can launch Hyperion Financial Management. DCOM sets the following controls:

1. Authorization level,
2. Determines who can launch HFM
3. Checks the identity of anyone trying to launch the application

DCOM enables network-based component interaction and enables sharing of processes across a network. With DCOM, components operating on a variety of platforms can interact, providing DCOM is available in the environment.

HFM SECURITY

HFM security is application specific and determines user privileges after launching HFM. There are three integrated methods to determine privileges:

1. Groups and Users within HFM, in our environment these groups mirror the network groups and individual passwords are the users' network passwords
2. Configuration Access which determines which tasks can be invoked by a group/user
3. Security Class Objects which determines data access. These classes are used to define and configure Process Management controls.

There are three production applications and each has been updated with the same security file. Since we will not implement Process Management in phase one, the only current Security Class is the Default Class. The Default Class for the groups and their inherent rights are outline below:

HFM_ADMIN
Have access to all aspects of all HFM applications. This includes the rights to change security privileges for other users and groups, delete and create applications and change any aspect of an application. This group is highly restrictive. Currently the members consist of two MBIA IT employees and the lead HFM consultant and a system domain id used to automatically load data into the applications.

HFM_FIN
Default Class set to ALL: User or group can modify data for elements assigned to the security class, and can promote and reject.
Configuration Access
Load System
Read Journals
Create Journals
Create Unbalanced Journals
Approve Journals
Post Journals
Journals Administrator
Review Supervisor
Submitter
Lock Data
Unlock Data
Run Consolidation
Run Allocation
Manage Data Entry Forms
Save System Report On Server

HFM_JOURNAL
Default Class set to Read: User or group can view data for elements assigned to the security class but cannot promote or reject.
Configuration Access
Read Journals
Create Journals
Create Unbalanced Journals

HFM_RPTDEV
Default Class set to Read: User or group can view data for elements assigned to the security class but cannot promote or reject.
Configuration Access
None

HFM_USERS
Default Class set to None: User or group has no access to any element assigned to the security class. User cannot promote or reject.
Configuration Access
None