A Hyperion White Paper

Introduction to Hyperion System 9 Security and User Management

This white paper provides an overview of the *Hyperion® System™ 9* security model. It also explains, in general terms, how *Hyperion System 9* manages users.

LDAP – Lightweight Directory Access Protocol is a software methodology for querying and modifying Directory Services, which acts as a layer between users and shared resources on a network. In a network, a directory identifies where in the network something is located. LDAP is a "lightweight" (smaller amount of code) version of Directory Access Protocol (DAP), which is part of X.500, a standard for Directory Services in a network. An LDAP directory is organized in a simple "tree" hierarchy and has entries to represent people, groups of people, organizational units, printers, or documents.

NTLM – NT LAN Manager is a security protocol, incorporated in a variety of Microsoft Windows operating systems for authentication purposes. NTLM uses an encrypted challenge/ response protocol to authenticate a user without sending the user's password itself. Instead, the system requesting authentication must perform a calculation that proves it has access to the secured NTLM credentials.

MSAD – Microsoft Active Directory is an implementation of LDAP Directory Services by Microsoft for use in Windows environments. Active Directory allows administrators to assign enterprise-wide policies, deploy programs to many computers, and apply critical updates to an entire organization. An Active Directory stores information and settings relating to an organization in a central, organized, and accessible database.

A key design objective for *Hyperion System 9* was to make the software easy to use, not only for business users, but for administrators as well. Part of this effort was building a common security layer spanning all modules of *Hyperion System 9*, accessed through a single interface—the *Hyperion System 9 Shared Services™ User Management Console™*. To deliver this significant, innovative functionality, a completely new user interface was constructed, and substantial work was also completed on the back end.

Authentication

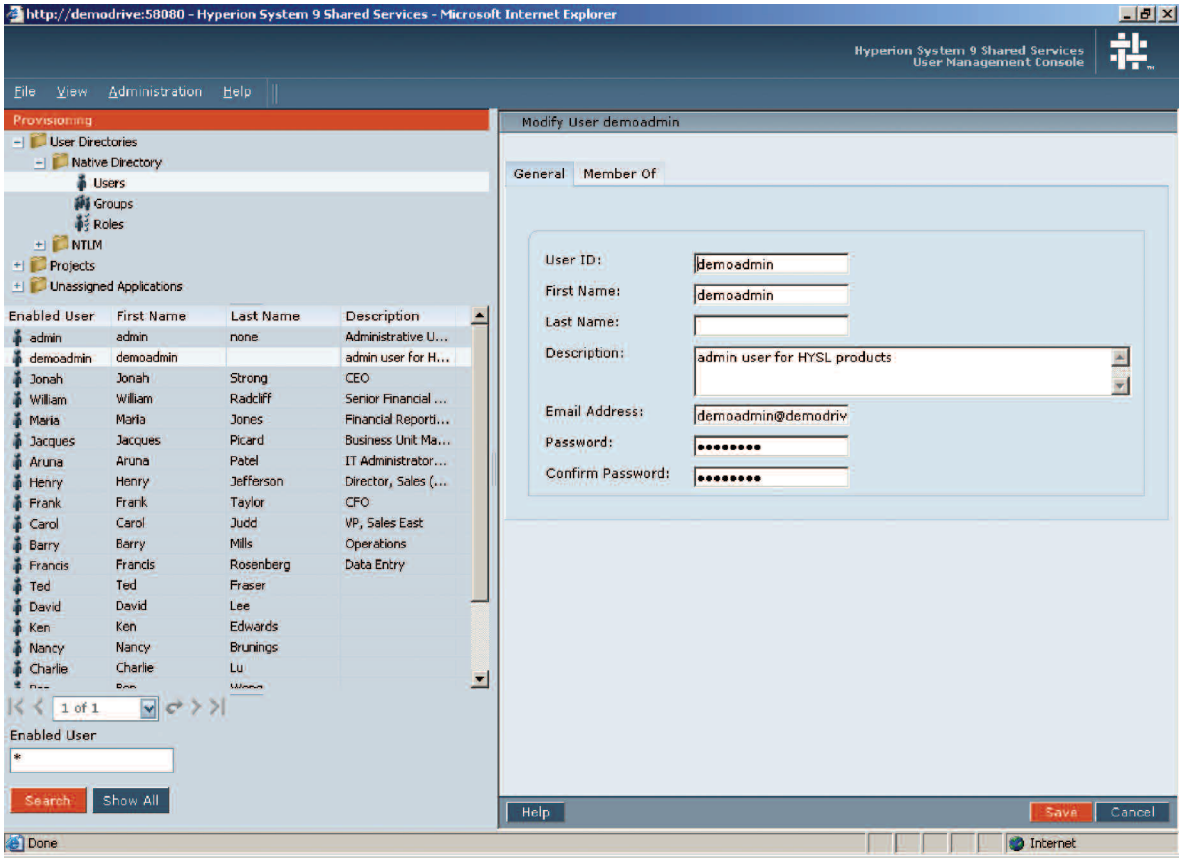
Authentication is the process by which *Hyperion System 9* attempts to confirm that a user is, or is not, who they claim to be. Many organizations already have a centralized authentication directory system in place, typically using technologies such as **LDAP**, **NTLM**, or **MSAD**. These directories are a centralized repository of user information, containing data such as usernames, passwords, groups, and access rights. *Hyperion System 9* has the ability to leverage these repositories to perform an external authentication. The term ***external authentication*** *means that the user's login information needed by* Hyperion System 9 is stored in these third-party directories.

These directories are stored outside of *Hyperion System 9*, yet it is unnecessary to import the user information into *Hyperion System 9*. If such a directory has not been set up within an organization, the native *Hyperion System 9* Shared Services, **OpenLDAP** directory (an Open Source version of LDAP), can be used to create and store user, group, and role information.

During installation and setup, *Hyperion System 9 Shared Services* is configured by a *Shared Services* administrator to gain access to these directories. When a user supplies their **credentials** (username and password) at login, *Hyperion System 9* accesses the user information stored in the external directory to authenticate the user in real time.

For administrators, having the ability to leverage their organization's existing security repository and managing all *Hyperion System 9* users from one interface significantly lowers their administrative burden.

Hyperion™
The future in sight



For business users, having a single user ID and password that will grant access to any or all of the applications within Hyperion System 9 is a welcome simplification. **Single sign-on (SSO)** allows a user access to multiple Hyperion System 9 applications after logging in only once. For single sign-on across all of your organization's applications, an **Identity Management** tool, such as Netegrity Siteminder, is required.

Authorization

Authorization is the process of finding out if a valid *Hyperion System 9* user is permitted to access the resource they are requesting. Examples of such a resource might be a report, a folder, or a database. If authentication is analogous to gaining access to an office tower, authorization is analogous to gaining access to a particular office once inside the tower.

When setting up *Hyperion System 9* for user access, a *Shared Services* administrator must define **Projects**. A Project is a folder that stores one or more *Hyperion System 9* applications. For example, a Project may contain a *Hyperion Planning*™ application and several *Hyperion Essbase*® applications. An application may belong to only one Project, and must be assigned to that Project before users can be provisioned. Once assigned, *Hyperion System 9* is ready to provision users and groups to the application.

Webster's dictionary defines the word "provision" as the act or process of providing; as well as the state of being prepared beforehand. **Common User Provisioning** is the process of preparing *Hyperion System 9* to provide access to users of the system, granting roles and access control. Based on roles assigned, users are allowed to perform specific tasks, and access only the content and reports

relevant to them, across *Hyperion System 9* applications. Provisioning is managed through the User Management Console, and is defined at the user or group level, that is, a Provisioning Manager selects users or groups and then assigns roles based on the specific application to be accessed. A **group** is a set of users that have the same security profile. A Group may also contain other groups.

The are six main steps to setting up security in Hyperion System 9.

Role Based Access Control

Each *Hyperion System 9* application has specific roles that may be assigned to either a business user or an administrator. A **role** defines the scope of activities a user can perform within *Hyperion System 9*.

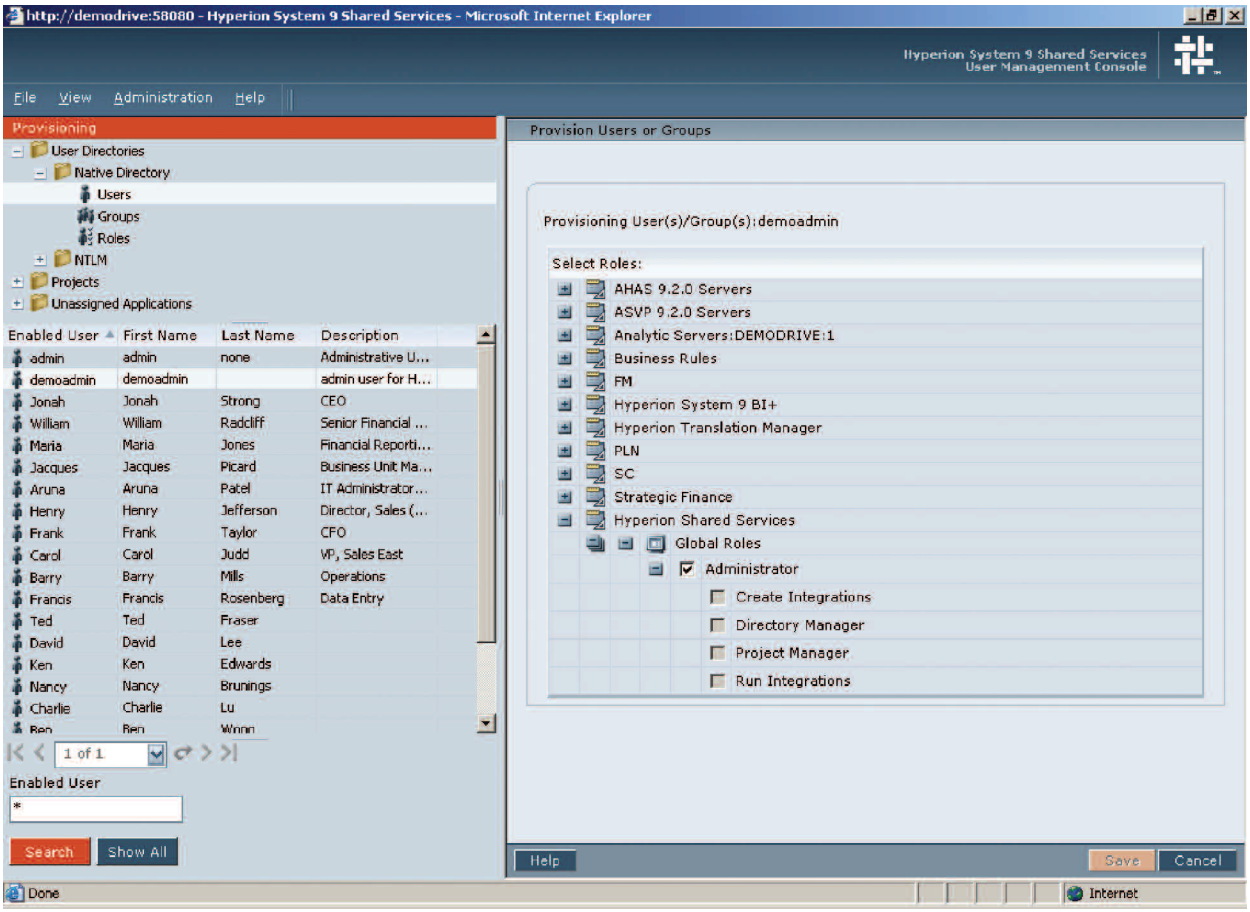
Administrative Roles

There are four global roles within *Shared Services*: Administrator, Directory Manager, LCM (Life Cycle Management) Manager, and Project Manager. In this way, administration tasks are spread across a number of administrators—without each having to be assigned the omnipotent Administrator role.

Hyperion System 9 is initially configured with one *Shared Services* Administrator. This is the most powerful role in the user management system and provides control over all installed *Hyperion System 9* applications. Administrators can perform all administrative tasks inside the User

Management Console, including provisioning themselves. If required, the Administrator has the ability to assign this role to other users. The administrator delegates security responsibilities to others by assigning them other, more restrictive *Hyperion System 9* administrative roles.

For example, Directory Managers have the ability to create, modify, enable/disable, and delete users and groups within a directory. A "hard" delete is only available when a user in defined in the *Hyperion System 9* native directory.



The Hyperion System 9 User Management Console allows you to delegate administrative tasks across different administrative users.

In addition, there are three other application-specific *Shared Services* roles: Provisioning Manager, Create Integrations, and Run Integrations. The Provisioning Manager may provision or de-provision both users and groups within applications. Provisioning Managers may not provision themselves, since their function is administrative only.

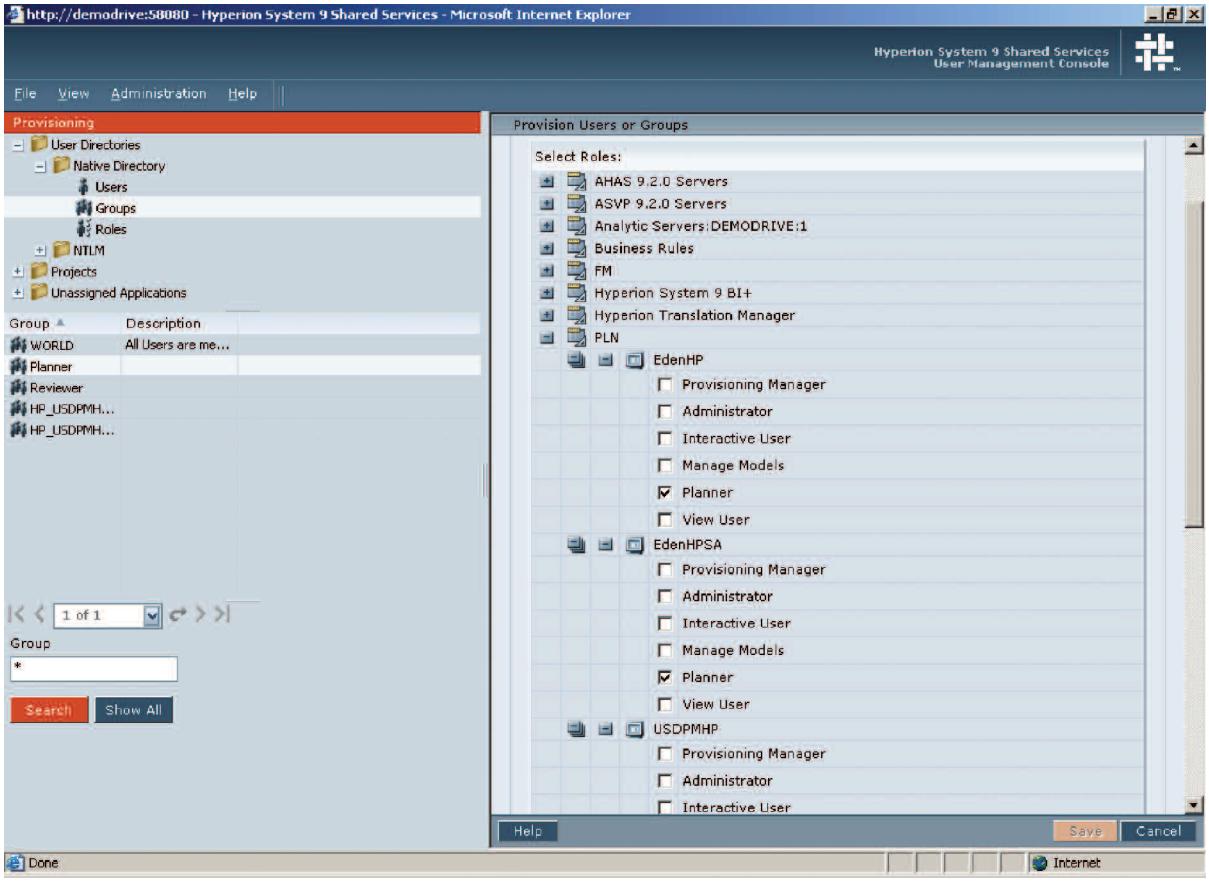
The *Shared Services* role allows you to move data between applications in what are called data integrations. The Integration role allows the user to perform actions on these integrations. The Create Integrations role can create and then manage the data integrations. The Run Integrations role can view, schedule, and run existing integrations.

Finally, *Shared Services* provides reporting that will allow an administrator a global view of all user role assignments across all Hyperion System applications, whether these assignments are direct or inherited.

Business User roles

Hyperion System 9 roles make it easy for the application administrator to set up security without having to involve corporate IT resources. This is accomplished through the *Hyperion System 9 Shared Services User Management Console*. Application-specific screens within this Console enable administrators to perform application-specific provisioning tasks. For example, the Provisioning Manager can set up users for access to dimensions within Hyperion Planning, specify the level of access, and determine which members and descendants to include.

The Planning application is packaged with four predefined user roles: Administrator, Planner, Interactive User, and View User. These are listed with check boxes in the User Management Console, which makes them straightforward to manage. The application Administrator, for example, performs all administrative tasks, such as creating applications and maintaining the metadata, managing security, initiating the budgeting process, creating and maintaining forms, etc. Planning allows for more than one administrator per application, which facilitates the delegation of maintenance across large applications. Custom roles can be defined by combining two or more roles.



Predefined user roles make setting up application specific security as simple as point and click.

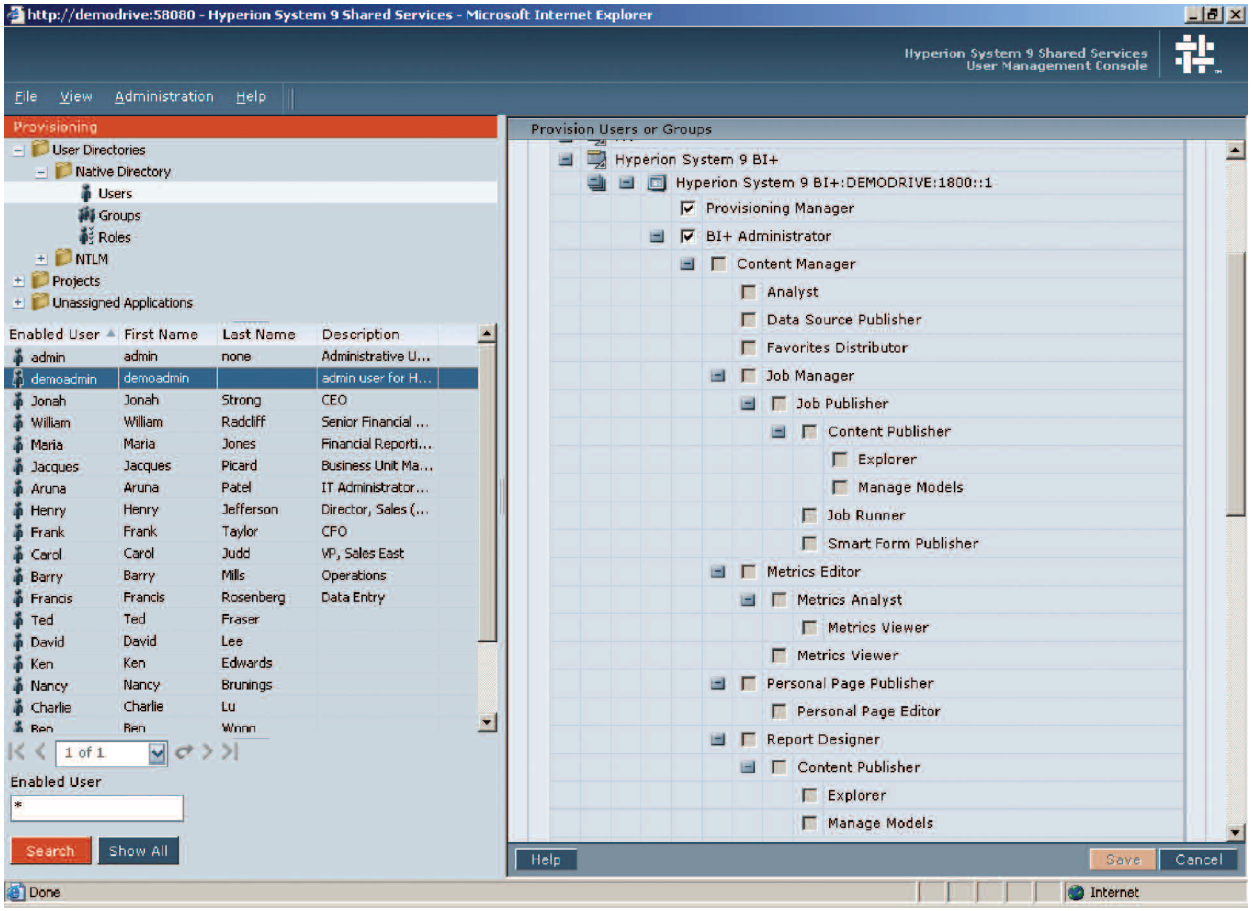
BI security extensions

Hyperion System 9 BI+™ Essbase Analytics™ and *Hyperion System 9 BI+ Enterprise Analytics™* are multidimensional database management technologies. Access is granted at both the server level and the individual application/database level.

Filter access allows security to be set on a database down to the most granular (cell) level. For *Essbase Analytics* and *Enterprise Analytics*, filter access can be granted to selected users and groups directly from the User Management Console. The filters themselves, however, must be defined within the application interface. This is one of the few exceptions in *Hyperion System 9* where the definition of security is only available within the application.

All *Hyperion System 9* reporting tools—*Hyperion System 9 BI+ Web Analysis™*, *Hyperion System 9 BI+ Financial Reporting™*, *Hyperion System 9 Smart View for Office™*, and *Hyperion Visual Explorer™*, as well as any custom or packaged applications that access data from an *Essbase Analytics* or *Enterprise Analytics* application—respect the security accesses imposed by the database.

For relational query and reporting, row and column level security can be enforced. This ensures that the data reflected in the generated result set adheres to this data-level security.



Hyperion System 9 BI+ provides a broad range of relational and multidimensional reporting and analysis capabilities. The User Management console contains sophisticated BI extensions that ensure your data is secure.

API and utilities

Hyperion System 9 has a fully published API that will allow for the programmatic assignment of user roles and access rights. This capability can significantly reduce the manual steps needed to give users access to resources, especially when there is a very large user base (tens of thousands of users), or when the corporate directory is housed within a custom data source. In addition, a bulk-load utility is provided to streamline the batch provisioning of large sets of users.

Conclusion

A key design objective for *Hyperion System 9* was to make the software easy to use. The implementation of an overarching *Hyperion System 9* security model is an important component in meeting this objective. Business users are issued a single user id and password that will grant them access to any or all of the applications they need within *Hyperion System 9*. Administrators are able to leverage their organization's existing security repository, and manage all *Hyperion System 9* users from one interface.

Hyperion Solutions Corporation Worldwide Headquarters
5450 Great America Parkway, Santa Clara, CA 95054
voice 1.408.588.8000 / fax 1.408.588.8500 / www.hyperion.com

product information voice 1.800.286.8000 (U.S. only)
consulting services e-mail *northamerican_consulting@Hyperion.com* / voice 1.203.703.3000
education services e-mail *education@Hyperion.com* / voice 1.203.703.3535
worldwide support e-mail *worldwide_support@Hyperion.com*

Please contact us at *www.Hyperion.com/contactus* for more information.

Hyperion™
The future in sight

6368_0906