Enterprise User Permission Management

PERMISSION_MGMT.1/10/20.11:30

TABLE OF CONTENTS

ENSURE SECURITY INSIDE AND OUT WITH PERMISSIONS

A top-down approach to security means recognizing insider breaches as seriously as those from the outside. Limiting access, or permissions, to only information or actions necessary to role will combat data breaches and infrastructural failure, an easy task for Futurex products such as the Key Management Enterprise Server (KMES) Series 3 or Guardian Series 3.

WHAT ARE PERMISSIONS?

Technology permissions do not trail far from their standard dictionary definition. Quite simply, permissions refer to the actions a user or group may take, not unlike the administrative or non-administrative privileges granted to PC users. In other words, permissions grant or deny users or groups access to a particular action such as changing passwords, loading Master File Keys (MFKs), or viewing logs.

Who has access matters. Trust is contingent to determining who has access to what, and trust has an inverse relationship to access. The greater the number of people with access, the lesser the degree of trust in a network. Home owners would not widely disseminate their house keys to strangers because they have little reason to trust them, and even less reason to trust so many of them. However, often, a stranger has nothing to do with the breach. Breaches often happen on the inside.

In fact, in 2013, Forrester released a report, "Understanding the State of Data Security and Privacy," in which a survey revealed that insider threats were the leading cause of data breaches between 2013 and 2014. Permissions play a vital role in preventing such breaches by limiting the ability of people within company walls to intentionally or unintentionally compromise data security and privacy.

Not all of such breaches are malicious attacks. Many may have been accidents such as a misplaced or shared password, but in a data-driven environment, accidents can lead to disproportionally severe consequences.

With tighter, more secure, permissions controls using Futurex technology, organizations can reduce the likelihood of data breaches both behind and beyond their walls.

THE PRINCIPLE OF LEAST PRIVILEGE

Organizations often seek opportunities to empower employees in order to give them opportunity to grow. Within the security infrastructure is not the place to do this. Information security professionals often adopt what is known as the principle of least privilege to protect from data breaches.

The principle is that individuals and groups should only have access to that which is essential to their role. For example, an auditor ought not to have access to the ability to do more than to view transaction logs. Having the ability to load, edit, add, or delete MFKs would not fit his or her role. In fact, to have that ability could compromise the integrity of the audit itself. It might seem convenient to give an employee administrative privileges, but it is dangerous if the employee does not need them.

Adhering to this principle helps to minimize the potential of employee mistakes or intentional breaches of data.

CONTROLLING PERMISSIONS

Administrators can customize permissions to fit organizational needs and adhere to the principle of least privilege using Futurex products such as the Key Management Enterprise Server (KMES) Series 3. The KMES Series 3 uses an intuitive Graphic User Interface (GUI) that allows ease-of-use. Adminstrators may set two different types of permissions: user and object.

USER PERMISSIONS

Like several Futurex products, the KMES Series 3 allows an administrator to create user groups with varying levels of access to server functions. Administrators, by nature of their roles, have full permission. When creating a group, users, with appropriate permission, have the ability to define the permissions set for a group and its users.

Once the set of permissions is defined for the group and the group created, the “owner” of the group, or creator, can create individual users who will derive their permissions sets from the parent group. In other words, when one creates a user within a group, he or she can only do as much or little as any other user in the group. Thus, a user in any group can never have more permissions than the group as a whole. In this regard, the KMES Series 3 inherently operates with a sense of the principle of least privilege, erring on the side of lesser permissions as opposed to greater.

SOME EXAMPLE ROLES AND PERMISSION SETS:

User permissions, as seen below, should be role-based.

Users	Group
	*Auditors* View Logs: ☑ Export ☑ Modify
	*IT Specialists* DatabaseBackup
	*Network Administrators* Manage Hosts/Networks: ☑ Add ☑ Delete ☑ Mass Import ☑ Modify
	*Key Management* Manage Keys: ☑ Add ☑ Delete ☑ Export ☑ Modify

OBJECT PERMISSIONS

Users with appropriate permissions may also set permissions for specific objects using Futurex products such as the KMES Series 3 or Guardian Series 3. Permissions can be set for the following objects:

- Reports
- Certificates
- Devices
- Hosts/Networks
- Keys
- Templates
- Users
- System Configurations
- Logs

Whereas user permissions define a set of actions a user can take, object permissions permit or deny access to acting on a specific object—meaning, even if a user has permission to view encryption keys, for example, that user would not be able to view keys for which object permissions have denied that user access.

Object permissions, then, are granular, allowing control of the least common denominators. By default, an object's owner group has full rights and all other user groups have none. Controlling permissions on specific objects ensures that users or companies working on the same network or device will not share access to sensitive information and actions. The least privilege principle cannot thrive in an environment where privileges are not so tightly controlled.

Users also have the option to set permission levels based on object type. This gives users the capability to define permissions on several objects simultaneously. Likewise, it allows them the opportunity to control which objects can have object permissions set. For example, one can set permissions for certificates to one of five permission levels: no object permissions, individual permissions, owner only permissions, or recursive individual permissions.

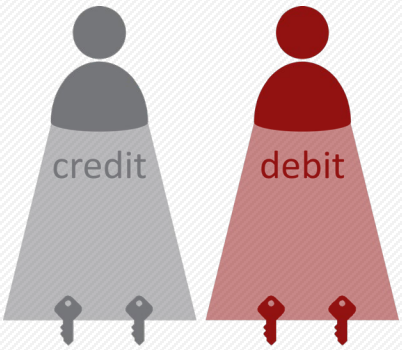
CASE STUDY

OBJECT PERMISSIONS IN PRACTICE

A major bank in North America using Futurex technology needed a way to separate credit and debit transaction and key management processes. Being separate, each department needed to ensure that it did not share access to specific keys and other objects while using the same key management servers. A user from the debit department, for instance, should not be able to view, modify, or delete keys accessed by users in the credit department.

They found a ready-made solution in Futurex's elegant object permissions features. By setting the object permissions to allow access only to specific users, such as the owner group, the two departments maintained a sophisticated permissions infrastructure that adhered to the principle of least privilege.

SAMPLE PERMISSIONS ACCESS FLOW



Users from both the credit and debit departments have the necessary user permissions to manage keys, but only the credit group has the object permissions to access the silver keys and the debit object permissions to access red keys.

GUARDIAN SERIES 3 INTEGRATION

Permissions management is even easier using the Guardian Series 3 because one can set permissions for all Futurex security devices in a network from one central GUI.

It is one thing to set permissions, but another to ensure that they remain up-to-date and safe. People change, positions change, and compliance mandates change among other things. Say an employee is promoted, and his role changes. Does this mean he should have more or fewer permissions? Neither. He should have whatever permissions he needs to do the job, meaning that, if he no longer needs the ability to manage keys, those permissions should be removed. Having the ability to set permissions on all devices from one central location ensures that an organization can keep up-to-date with organizational changes.

Because an administrator can use the Guardian Series 3 to manage all Futurex devices in the network, periodic reviews of permissions are quick and easy. This means that permissions can not only be set using best practices but maintained as well.

Data breaches can cost millions, in some severe cases billions, of dollars. Protecting that data depends on many factors—one of which is permissions control. Managing permissions properly is one more step toward safety and profitability.

About Futurex

For over 40 years, Futurex has been a globally recognized name in providing secure, scalable, and versatile data encryption solutions.

More than 15,000 organizations worldwide have trusted Futurex's innovative hardware security modules to provide market-leading technology for the secure encryption, storage, and transmission of sensitive data.

Futurex maintains an unyielding commitment to offering advanced, standards-compliant data encryption solutions alongside world class customer service.

FUTUREX ENGINEERING CAMPUS
OFFICE: +1 830 - 980 - 9782 TOLL FREE: 800 - 251 - 5112
864 OLD BOERNE ROAD, BULVERDE, TEXAS, USA 78163