Best Practice Guide to Implementing the Least Privilege Principle

Enter Your Business Email

Download Free Guide (.PDF)

We never share your data. Privacy Policy

Principle of Least Privilege Benefits

The principle of least privilege (POLP) requires giving each user, service and application only the permissions needed to perform their work and no more. It is one of the most important concepts in network and system security. No matter how technically skilled or trustworthy a user is, they should have access to only the network resources they need to do the job at hand.

The main benefit of minimizing each user’s level of access is that you can dramatically reduce your security risks and attack surface. By strictly limiting who can access your critical systems, you reduce the risk of unintentional or malicious changes and data leaks — whether by the users themselves or by attackers who take over their credentials. In particular, you’ll minimize the likelihood of rootkits, viruses and malware being installed, since most user accounts won’t have the administrative privileges required to install them.

Another benefit of enforcing least privilege is achieving regulatory compliance. Many standards require organizations to give users only the privileges needed to complete their job functions — especially privileged users. Even if your business is not subject to these the system's configuration could be changed inappropriately, either deliberately or accidentally. Least privilege helps you maintain the intended configuration of a system by controlling exactly who can change what. Great examples of administrative restrictions that implement least privilege are the ESAE ("Red Forest") model in Active Directory and the Just In Time and Just Enough administration concepts in Windows Server.

Limitations of Least Privilege

However, it's essential to keep in mind that the principle of least privilege is just one layer of a comprehensive defense-in-depth strategy; you should also deploy other critical technologies, such as firewalls that prevent connections, intrusion detection devices that search for malicious code, antivirus or personal security products that look for heuristic behavior, and software restriction policies that limit what application installation and execution. For example, suppose a user has a legitimate need to access certain sensitive data. If keylogging software is installed on that user's machine, that data could be transmitted to a third party without the user's knowledge. The least privilege principle alone will not block this attack path, since the user needs the access rights, but a comprehensive defense-in-depth security strategy would almost certainly prevent the data breach.

Understanding Types of Accounts

To implement the principle of least privilege, you need to set up different types of account for different purposes. These include user accounts, privileged accounts and shared accounts:

- **User accounts** — Most people in your network should get a regular user account with the access required to perform their normal duties.
- **Privileged accounts** — A privileged account with elevated privileges. There are two main types. The first is accounts that enable specific users, such as accounting executives, to access critical data and services. The other is administrator accounts, which grant special admin rights on the network. Classic examples include the root account in Linux and administrator and power user accounts in Windows operating systems. In a Microsoft environment, the most important administrative account is the Domain Admin account. While a local admin account grants complete control of a single

closely controlled. In general, administrators should have both a user account and a privileged account, and they should use their least-privileged user accounts unless they need to perform a specific task that requires their administrative privileges.

- **Shared accounts (generic accounts)** — Using shared account is usually not recommended; the preferred method is to have each individual use their own account. However, in some limited situations, it may be acceptable to create accounts that are shared among a group of users. For example, most organizations of any significant size have outsiders who need to access their network, such as clients, contractors or business partners who are visiting for a brief period of time. Creating guest accounts with bare minimum privileges can be an expedient way to enable these users to complete basic tasks.
- **Service accounts —** Humans are not the only entities that might require privileged access to network resources. You might have software that needs to access your network without human intervention, such as database services that start when their machine boots up. These services require their own accounts. One common but dangerous practice is to assign these services to a Domain Admin account. If attackers compromise an application that is running as a Domain Admin, they immediately get administrative access to the system. Application security best practices require organizations to determine what access each application requires to run correctly and create service accounts with just enough privileges for the applications to accomplish their required tasks; limiting the access that applications have to your network will go a long way toward protecting it from abuse. Active Directory provides a service account with a very strong password that is automatically changed.

Managing Passwords

Regardless of the type of account, credentials best practices recommend enforcing certain controls on passwords, including the following:

- **Password length —** The longer the password, the better. Passphrases are becoming more common.

- ✓ **Password age** — Passwords should expire and have to be reset after a specific number of days.
- ✓ **Password history** — The system should remember a certain number of previous passwords for each user to prevent their immediate reuse.

You can read more about passwords and their settings in password best practices.

You should also apply an account lockout policy, as detailed in account lockout best practices.

Deleting Accounts

When someone leaves the company, for any reason, that user’s accounts should be disabled immediately, and then deleted after a period of time. If you delete the account immediately, you might not be able to access important data, and you might even lose some logs associated with the account. You can get more information in user termination best practices.

Privilege Management

Using Groups

Trying to manage privileges individually for hundreds or thousands of employees and adhere to the principle of least privilege is a difficult task. A better access control strategy is to place users into groups based on their job roles and then to manage privileges for those groups. For example, suppose your company invests in a new HR application. Instead of having to grant each HR staff member access to the application individually — a time-consuming and error-prone task — you simply give the HR group the appropriate permissions. Similarly, if a user transfers from one department to another, you can simply remove them from certain groups and add them to others, rather than having to manually remove dozens or hundreds of specific access rights and add a similar number of new ones.

Assigning User Working Hours

For employees who work a relatively consistent schedule, another layer of least privilege is to

Using Location-based Restrictions

In many cases, you can also limit which locations an account can be used from. For instance, an account might work fine in the San Francisco office but not work at all from the Los Angeles office.

Using Machine-based Restrictions

Machine-based restrictions are a special type of location-based controls. For instance, you can keep a user who works in the Accounting department on the 4th floor from using machines on the 10th-floor software development area. Again, not all accounts can be locked down like this; for example, some technical support personnel might need to be able to work from almost any computer on the network.

Secure Configurations

Each system should also be configured so that it is capable of doing only what it is intended to do and no more. Best practices for locking down systems including changing all default passwords and disabling any default accounts and services you don't use. After all, a simple Google search is all it takes to find the default username and password for any system but changing those credentials is an easy task, and simply shutting down anything that you don't need will go quite a long way to improving computer security. It is amazing how often real-world system audits turn up systems with default usernames and passwords — even backbone gateway routers or storages with sensitive data that should be password protected and have multifactor authentication implemented.

Auditing Accounts

Setting up the right accounts, assigning them the appropriate privileges and applying any applicable restrictions is a good first step. However, you also need to audit those accounts periodically. Tree types of audits are relevant to accounts: usage audits, privilege audits and change audits.

- ✓ **Usage audits** — It's critical to monitor what each account is doing, including what data they access, create and delete. Regular review of this data helps you assess whether the

- **Privilege audits** — Over time, users can end up with privileges that they no longer need. This can occur when the user's job role changes and new privileges are simply added to the old ones; other times, users are simply provisioned with more privileges than their job role actually required. Regular privilege audits help you spot accounts that have more privileges than required so you can enforce least privilege. Privilege audits are closely related to recertification, which is the process of working with data owners and users to determine if given accounts still require the privileges that they have.
- **Change audits** — Any improper change to an account's password, permissions or settings could lead to a data breach. Therefore, you need to be sure that all changes are under your full control and you are alerted about all critical changes.

Usage, privilege and change auditing can be automated by third-party tools like Netwrix Auditor, which will report on all changes in your environment and alert you about changes you deem critical, such as changes to administrative group membership.

Conclusion

Applying the principle of least privilege is hard, even for organizations with high incentives to be secure. It requires constant testing of security boundaries and the monitoring of privileged access. But the benefits are huge: It will help you defend against external attacks and insider threats, comply with regulatory requirements, and simplify change and configuration management.

Previous

Next

Related best practices

★ Password Policy Best Practices

★ Account Lockout Best Practices

Netwrix Auditor

- Platform Overview
- Request a Price Quote
- Solutions
- Virtual Appliance
- Cloud Vision

Netwrix Freeware

- Free Netwrix Auditor for Active Directory
- Account Lockout Examiner
- Top 7 Free Tools

Audited Systems

- Active Directory
- Azure AD
- Office 365
- Windows File Servers
- EMC
- NetApp
- Windows Server
- Exchange
- SQL Server
- Oracle Database
- VMware
- SharePoint
- Nutanix Files

Compliance

- PCI compliance
- HIPAA compliance
- SOX compliance
- FISMA compliance
- ISO 27001 compliance
- GLBA compliance
- FERPA compliance
- NERC compliance
- GDPR compliance
- CJIS compliance
- CCPA compliance

Online Help Center
Support Programs
Knowledge Base
Submit Ticket
Customer Portal
Renew Maintenance
Freeware Support

About Us
Contact Us
Our Customers
News

Privacy Policy | EU Privacy Policy | EULA

Corporate Headquarters: 300 Spectrum Center Drive,
Suite 200 Irvine, CA 92618

Phone: 1-949-407-5125 | **Toll-free:** 888-638-9749

Select region ▾