A guide to

Instant Privilege Access

Learn more about Instant Privilege Access and what benefits it brings in terms of productivity and security

UPKEEPER

Table of Contents

Instant Privilige Access

In this whitepaper we discuss a challenge that many organizations face; to maintain maximum security for its client computers while giving users the opportunity to manage their computer themselves.

We have found that awareness of the problem is low, and many organizations have solved it by allowing all, or far too many, users to have admin rights, which opens up for malware and other vulnerabilities. Others completely lock down all client computers, degrading the user experience and burdening IT support with routine tasks.

Today's solutions, often called Privileged Access Management ("PAM"), can be complex and expensive to implement, preventing IT and management from being in control.

Instant Privileged Access (IPA) is a new category of solution that focuses on managing a user's own admin rights in a simple, cost-effective and secure way.

We go through technical challenges with client security, scenarios and problems that need to be addressed and how an IPA solution can handle this.

Client computers and their users are one of the biggest the security risks in an IT system.

IT and computer security is one of the highest prioritized areas for all companies and organizations.

The usage is becoming more and more personalized, i.e. that you want be able to adapt their software set and computer so that it suits thier way of working and their workplace. Remote work is increasing which makes access to users' computers more difficult.

The companies must cope with these opposing demands with a good user experience and without increased costs for IT support.

IPA

Instant Privilige Access (IPA) specifically addresses this through giving users the right to make predetermined changes themselves without delay, even if the change temporarily requires admin rights. The company can control which changes are allowed and get full traceability, without burdening the IT department.

Comprehensive understanding of client computer security

Computers managed by a user who is a local admin are significantly more vulnerable to intrusions and malware and require more maintenance, but have the most satisfied users.

To better understand why privilege access is important in a larger security perspective, we must first understand the current threat to the users of client computers. Here we will look at the different extremes when it comes to how client computers are configured and connected and show their different pros and cons from a security perspective. We also take productivity and user satisfaction into account.

In the graphic on the next page, you can see that the client computers that are not managed and used by local administrators are the ones that are the most flexible and when it works, and they also have a very high user satisfaction.

Studies also show that computers that are continuously used by local administrators run a much higher risk of being infected by malicious code, while also requiring more support and maintenance over time.

Scenario 1

Research and control of simpler units

Admin, no internet access

No external access

High security level

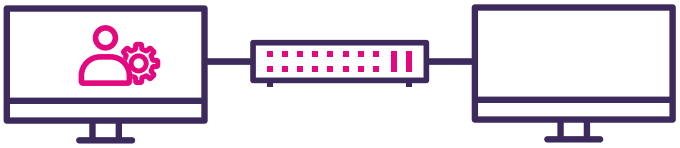
Scenario 2

Computers that manage other units

Admin, closed network

Limited exposure

High security level



Scenario 3

Office computer that is managed

User

Managed and updated

Average security level

Scenario 4

Office computer that can be managed

User and admin when needed

Flexible usage with control

Average secutity level

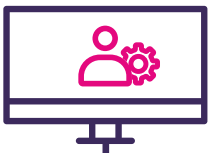
Scenario 5

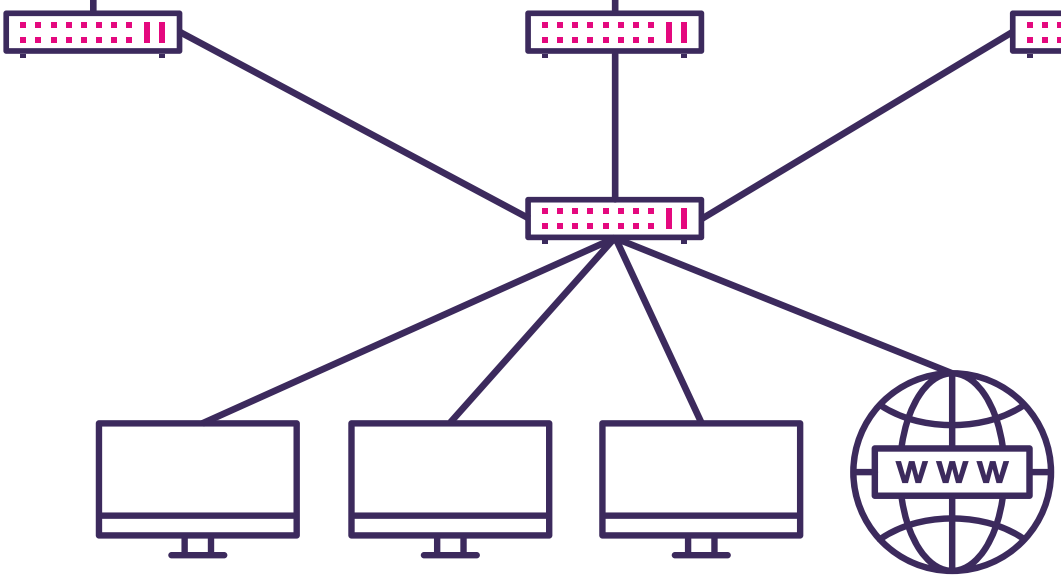
Home computer

Admin

Flexible usage

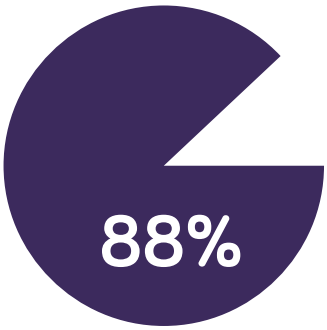
Low security level





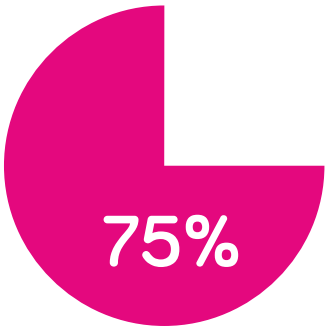
“I have multiple customers who have decreased the number of tickets to their service desk by a whopping 75% by getting rid of end-user admin rights.”

Sami Laiho, Windows OS & Security Expert, Senior Technical Fellow



Share of asked organizations that consider inside threats a cause for concern[1]

The number of Microsoft vulnerabilities in the category “Elevation of Privilage” 2022 which now stands for more than half of all Microsoft vulnerabilities[2]



Proportion of critical Microsoft vulnerabilities which can be mitigated by removing admin rights[2]

1 ENISA Report Threat Lancscape 2020 | 2 Beyond Trust: Microsoft Vulnerabilities Report 2023

Creating completely secure client computers is not impossible, but is in most cases linked to reduced productivity and user satisfaction.

Best Practice - give the user the least possible admin rights

Best practice, from a security perspective, says that a user should have as few rights as possible at any given time. But without flexibility, user productivity and user experience are hampered.

There are many of us who advocate that users and applications should always be given as limited rights as possible and only to the resources that are to be used. This means that users and applications must have as few rights as possible to the resources they use in the continuous workflow.

If a user or application needs extended rights to existing or other resources from time to time, they shall only be assigned temporarily and under controlled conditions.

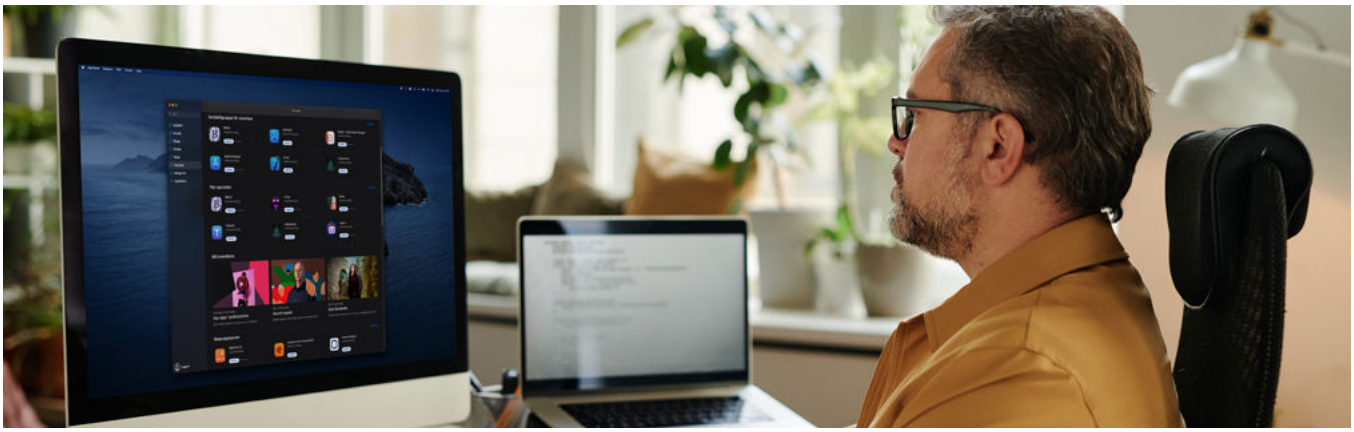
Giving users or applications higher rights or access to resources they do not need creates unnecessary risk both in terms of security and mistakes.

A knowledgeable user with too many admin rights

User Erik needs some applications that only he uses and has access to. The applications are not part of the company's standard set, but are important for Erik's work. The IT department does not have knowledge of these and does not receive notifications about updates etc.

To make it easy for Erik to maintain the applications, they have chosen to let Erik be the administrator on his computer. Because Erik is an administrator on his computer, he can maintain the applications on his own and the IT department does not need to be involved.

Erik is knowledgeable. But because he is an administrator, it also means that he can install other applications that he chooses himself, but also applications or scripts that he starts by mistake or that are delivered covertly via email or web pages. Here the problems begin.



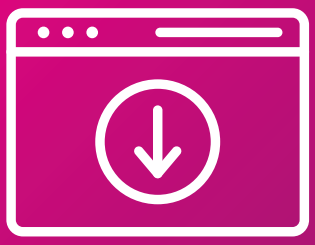
Being a local administrator provides increased freedom and flexibility for the user, but it also creates an increased exposure in terms of security.

The example above may seem trivial, but it is a clear violation of the principle of least access and is all too common. To give the user the flexibility required, far too many organizations allow all or many users to have elevated privileges permanently. The problem is not only what these users can do, but also the fact that there is no traceability of what has been installed or happened on the computer.

The fact that the user is not a local administrator on a day-to-day basis is the safest option for both the organization and the individual user. If you are a local administrator in your daily work, the risk of making your computer unusable increases. Accidentally or via malicious code obtained via email, web or other external sources. If you are a local administrator, the risk of malicious code getting on to other devices such as computers, tablets, phones, servers and functions that are connected to the same network in the organization also increases.

User scenarios - what problems need to be solved?

To be effective, a solution that addresses least privilege must be able to handle several different activities, actions, and situations. It is both about what the user should be able to do, but also where or in which user scenario the action should be performed.



Installation of application

A user who needs to install an application that is not in the organization's managed application directory but is approved, must in a managed environment turn to the organization's IT function. They in turn may log in locally or remotely with elevated rights to install the application. This comes with a lead time and the user will have to wait for the installation to complete.

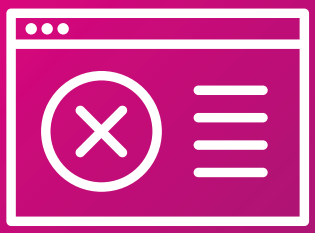
For the person from the IT function who implements the change, this will take unnecessary time as they probably do not know the application itself and its function, which can create many questions and in the worst case an unusable installation due to misconfiguration.

If the user themself could request temporary local administrator rights configured to approve only the installation of the specific application from a specific location, the installation could be carried out safely and possible configurations could be to the user's advantage.

Network issues

A user experiencing problems with their network configuration must in a managed computer environment, always leave the computer to the organization's IT function, which can remedy the error. Giving away the computer is often costly both in lost production and user satisfaction, but can be necessary in some cases.

If the user could request local administrator rights and get guidance from the IT function in the organization you will be able to reduce production loss and user frustration.



Troubleshooting

A user who experiences problems with their computer and contacts the organization's IT function for help often does not have the right to troubleshoot their own computer on the level required. In some cases the IT department can help remotely, in other cases not.

If the user is a regular user on a daily basis but can request temporary local administrator rights that are predefined by the organization's IT function, the risks of mistakes and running off malware are minimal. Any process that is started in administrator mode must be confirmed by the user entering their login credentials which can be username and password, pin code, facial recognition or any other login feature that authenticates the user. Once the user has obtained local administrator rights, they can by themself, or with the guidance of the organization's IT function, troubleshoot the computer and hopefully solve the problem that has arisen.

What is Privilege Access Management?

PAM often addresses the problem as such but not all user scenarios. PAM solutions also cover many other aspects, which makes implementation and use complex and the solutions expensive.

Privilege Access Management is about being able to control and monitor extended rights regarding users, accounts, processes, applications and systems in the entire IT environment. The purpose of Privilege Access Management is to reduce the exposure purely in terms of security for the user and the organization, but also to follow the events so that it is only used according to what has been decided.

Implementing Privilege Access Management systems is in most cases complex, time-consuming and expensive. It can take months of planning in a larger organization where many people become involved to understand exactly what needs to be handled during implementation. As systems are often extensive and for the uninitiated relatively complex, external resources are often required who first have to familiarize themselves with the business before they can help with the strategic work and then the actual implementation. This means that it is not only the system itself that is often expensive, but it also results in high consulting costs that often far exceed the actual system cost.

In many cases, systems are used primarily to assign and control elevated rights for users and special accounts. In these cases, the user requests elevated rights to be able to implement any type of change that requires this. The request is then handled manually by people or automatically via a predefined set of rules.

Introduction to Instant Privilege Access

Instant Privilege Access ("IPA") specifically addresses the need to be able, when necessary, to grant a user temporarily elevated privileges in a secure, controlled, and automated manner. Since IPA focuses on this, it becomes a solution that is simpler and more cost-effective to implement compared to, for example, a PAM solution.

Instant Privilege Access is a function where users can immediately upon request be given elevated rights to a specific device based on a predefined set of rules. Once the user has received the rights, they can perform actions on the device based on the regulations and everything performed is logged. The increased right is restored within a defined period. The process does not require intervention from e.g. the IT-department.

Instant Privilege Access is a sub-function of Privilege Access Management where the focus is on security, simplicity and user satisfaction. The function must be able to be activated regardless of where you are, i.e. it should work whether you are in the office, at home or on the go. It must also work with or without access to a local network or the Internet. In addition to being able to request access regardless of where you are, the function must give the user direct feedback as to whether access has been granted or denied.

This means that a user who requests rights will be authorized directly based on the predetermined regulations and thus be able to carry out what they are entitled to. The direct access promotes productivity where the user can immediately complete the desired task without the involvement of other resources. When the user has completed their changes, the elevated right is revoked and the user regains their normal rights.

Everything that the user starts with their elevated rights must be confirmed with some form of validation, which can be username and password, pin code, facial recognition or any other login function that confirms the user. What is carried out with elevated rights must be logged separately so that the measures can be monitored and analyzed. Analysis and changed needs can lead to adjusted rights for individual users or the entire organization and must take place immediately upon change.

With Instant Privilege Access, exposure is reduced in terms of security as the user must actively initiate the change and approve it by entering login information. The fact that the user has elevated rights for a limited time also results in reduced exposure.

upKeeper Instant Privilege Access

upKeeper IPA allows an organization to grant selected users or groups predetermined elevated rights with full control and traceability as described above. The solution is as easy to implement as a regular application and requires no changes to processes or policies.

upKeeper Instant Privilege Access is an implementation of Instant Privilege Access where we have stuck to the core values and focused on security and usability. With upKeeper Instant Privilege Access, users are given the opportunity to easily request elevated rights according to a predefined set of rules that work regardless of where the user is and regardless of internet connection access.

When you as a user have been granted elevated rights, you can carry out approved tasks such as installing an application or making changes a registry value. Once the task has been completed, the rights are revoked and the user

cannot therefore carry out more changes with elevated rights. The user can again request increased rights if the need arises. Everything that the user carries out with elevated rights will be logged so that you can follow it immediately or analyze it afterwards.

In addition to the advantages that upKeeper Instant Privilege Access provides from a security perspective, there are other advantages for both users and IT support, which benefits the entire organization.

For the IT support, the function provides better control and the possibility of follow-up. You can give different user groups or individual users different possibilities for changes based on needs. When needs change, you can easily adjust the possibilities for the user group or the individual the user.

For users, the function gives the opportunity to make changes when they need them, regardless of where they are. The function is activated by the user who also needs to verify their login details via an activated login function, which can be a password, card, pin code, fingerprint or facial recognition. This procedure allows the user to feel confident that only functions they actively start run with elevated privileges.

For the organization, the feature reduces the burden on IT support, which can take on other tasks, and users can do more when it suits them. Over time, you will see that productivity increases, which can be linked to happier IT support employees and the user group who become more flexible and safer.

1. The user requests admin rights through upKeeper IPA

2. IPA grants the user rights according to predefined policies

3. The user makes changes and tasks that are logged by IPA

4. Admin rights expire after one predefined time or number of actions

5. The user no longer has admin rights

To implement upKeeper Instant Privlege Access

Rolling out traditional Privilege Access Management (PAM) systems can be time and resource intensive in larger organizations as they require careful planning and extensive configuration.

Rolling out upKeeper Instant Privilege Access is as quick and easy as installing a regular application.

1. Create a user account in the upKeeper Instant Privilege Access portal.
2. Create an initial configuration of who should have which rights.
3. Download the client application.
4. Roll out the client via a client management system such as upKeeper Manager, Microsoft Intune, Microsoft System Center Configuration Manager or similar.
5. Monitor usage and make necessary adjustments.

The implementation process is simple and usually takes a couple of hours from registration to rollout, but updating or creating a security policy can take longer depending on the organization

Do you want to learn more?

Do you want to learn more about upKeeper Instant Privilige Access?

More information

Contact me

About us

upKeeper is created for IT service providers and organizations with their own IT function. Since 2008, we have been delivering systems for client management and also specific solutions in guaranteed recovery, admin rights management and energy saving for computers. We give users more freedom and increased productivity while you retain control and get the ability to quickly recover from an attack. More than 100,000 clients are currently managed by our solutions.

upKeeper Solutions AB
Tvistevägen 48
907 36 Umeå Sweden
www.upkeeper.se/en
090-349 33 90