ManageEngine
PAM360

SERVICE ACCOUNTS 101

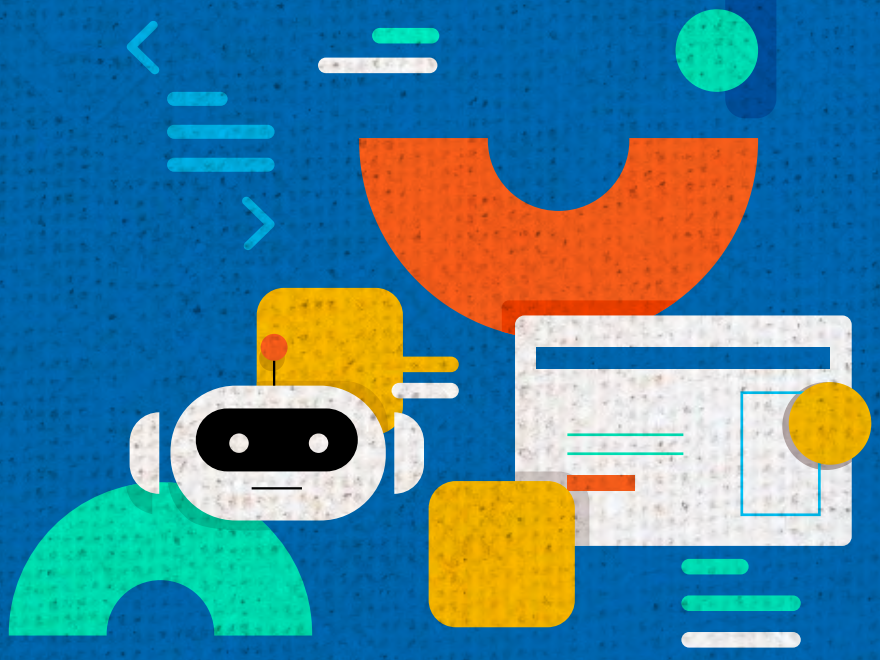


Table of contents

Introduction

Why is it that when a computer boots, certain applications and processes start along with it by default? Or, we might wonder, have they ever stopped functioning in the first place? Typically, the system's clock, calendar, task manager, or applications like antivirus software, website browsers, or the system's AI, be it Bing, Siri, or Google, start-up along with the machine. Why does this happen, how does this happen, and is it necessary?

For starters, this is made possible by service accounts.

This white paper will dive into the intricacies surrounding service accounts and their functions in a full-scale enterprise IT network, while taking a closer look at the purpose behind its adoption.

What are service accounts?

Any soft process that runs on a computer, at its core is a service, be it applications, protocols, algorithms, etc. Services are the atoms that makeup an interactive user interface. All processes ranging from system time and calendar to network protocols and admin functions, all of them are packaged as services that are executed by user accounts. These accounts are essentially called service accounts.

Service accounts are unique, non-human user accounts that are assigned privileged access to perform background services. These services include everything that builds up to the user experience from low-level calculations, file transfers, application functions and all the way up to high-level tasks like automated administrative services, establishing virtual machine connections, and other security operations that involve critical usage.

Human user accounts vs. service accounts

Generally, for a process to run on a computer, a user is expected to login to that computer and execute the process. To do this, user accounts are created for human users to log-in to the system and execute the process.

Similarly, to run a background process that ideally does not require any user involvement, in other words a service, a service account is used. These accounts are also user accounts, but they are not accessed by human users. Service accounts tagged to particular services to automate them.

Built-in Windows service accounts

Windows services are typically managed by a central tool called the service control manager (SCM). The SCM utilizes built-in service accounts to execute these predetermined Windows services that are hard coded into the system's functionality during OS installation.

The user accounts that are used to run a service on a Windows environment are commonly known as Windows service accounts. Running in the background are numerous predesigned services that essentially make up an end-user's UI. An end user is not expected to create these service accounts themselves, especially since not all end users are technically sound enough to do so.

How do these services run and which account handles them?

To optimize a common user's UI experience, there are built-in Windows service accounts that are created during OS installation. They have different properties and they are used to execute various services. When the Windows OS is installed, by default it creates three service accounts to run background processes that don't necessarily require user intervention to run. These service accounts are not displayed on the user manager, but by default belong to the Administrators group and have access to all files within the Windows NTFS.

1 Local System account:

This is a built-in local service account with high-level admin privileges for that particular machine. This account does not function using eternal passwords. It utilizes the default password stored on the hard drive during OS installation. A local system account belongs to one particular system or mainframe and performs no network related services.

2 Network Service account:

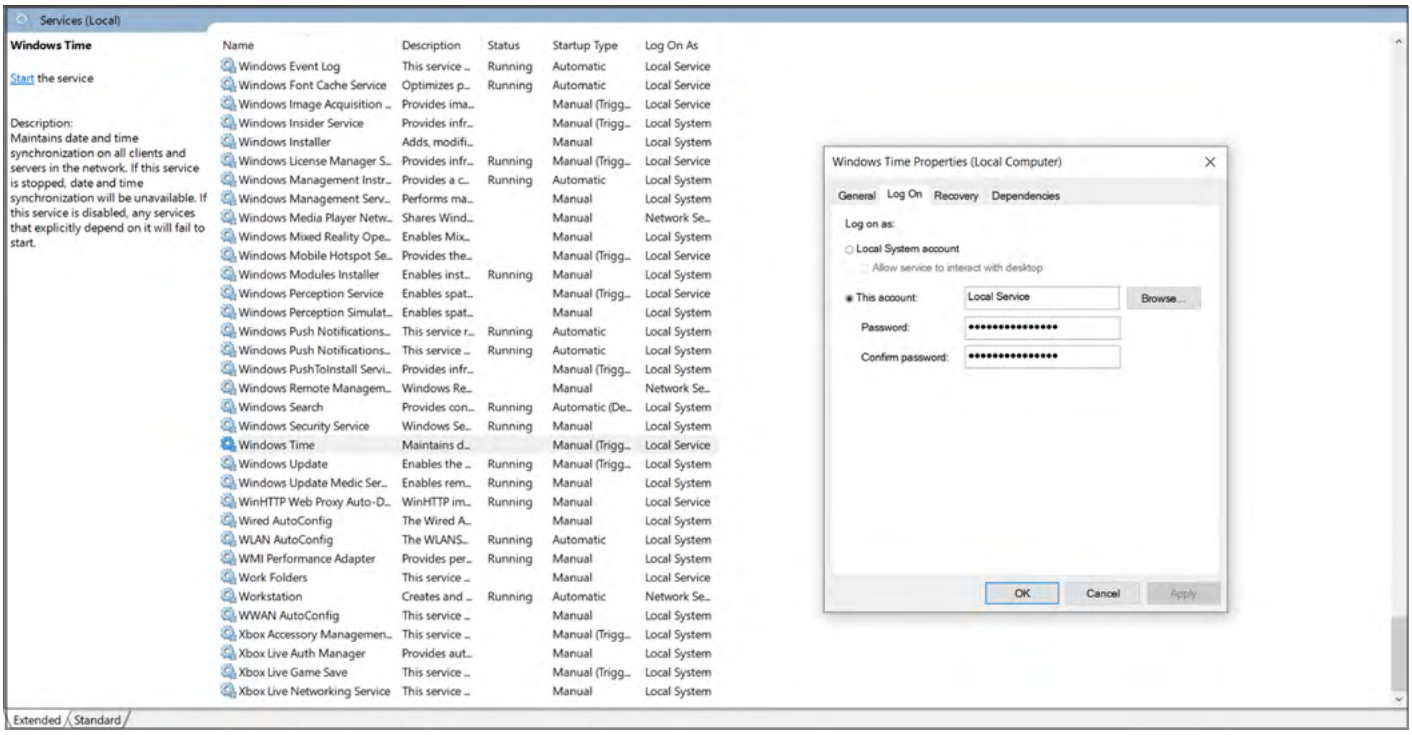
This is a predefined service account used by the SCM to perform services. However, as the name suggests, a network service account is used to perform network services with its corresponding server. A service that is handled by the network service account tends to display the system's credentials on remote servers.

3 Local Service account:

This is also a predefined service account used by the SCM to perform service and functions differently form a network service account in only one way. A service performed by the local service account does not present the credentials of the computer to remote servers and requires special permissions to do so.

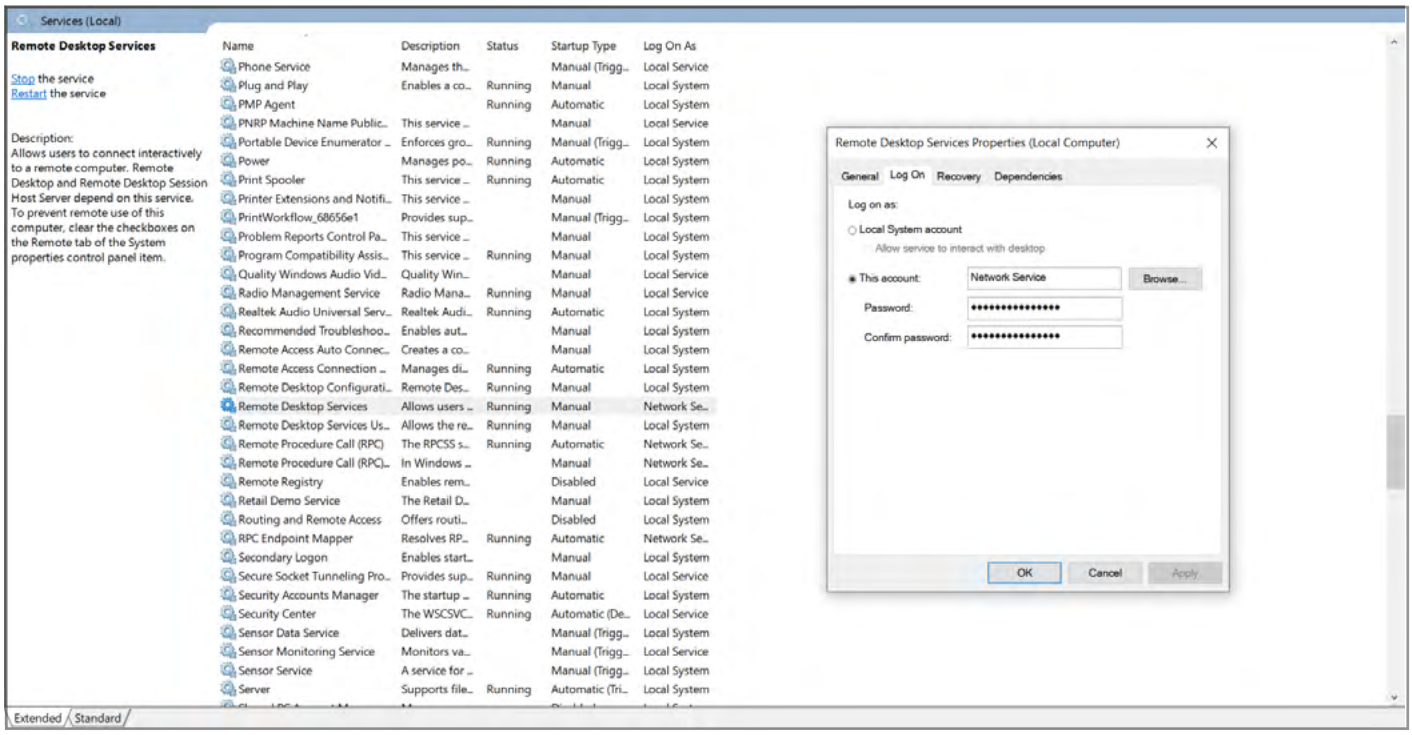
Let us try to understand built-in Windows service accounts with the following service examples. These examples are taken from the SCM.

Local Service account



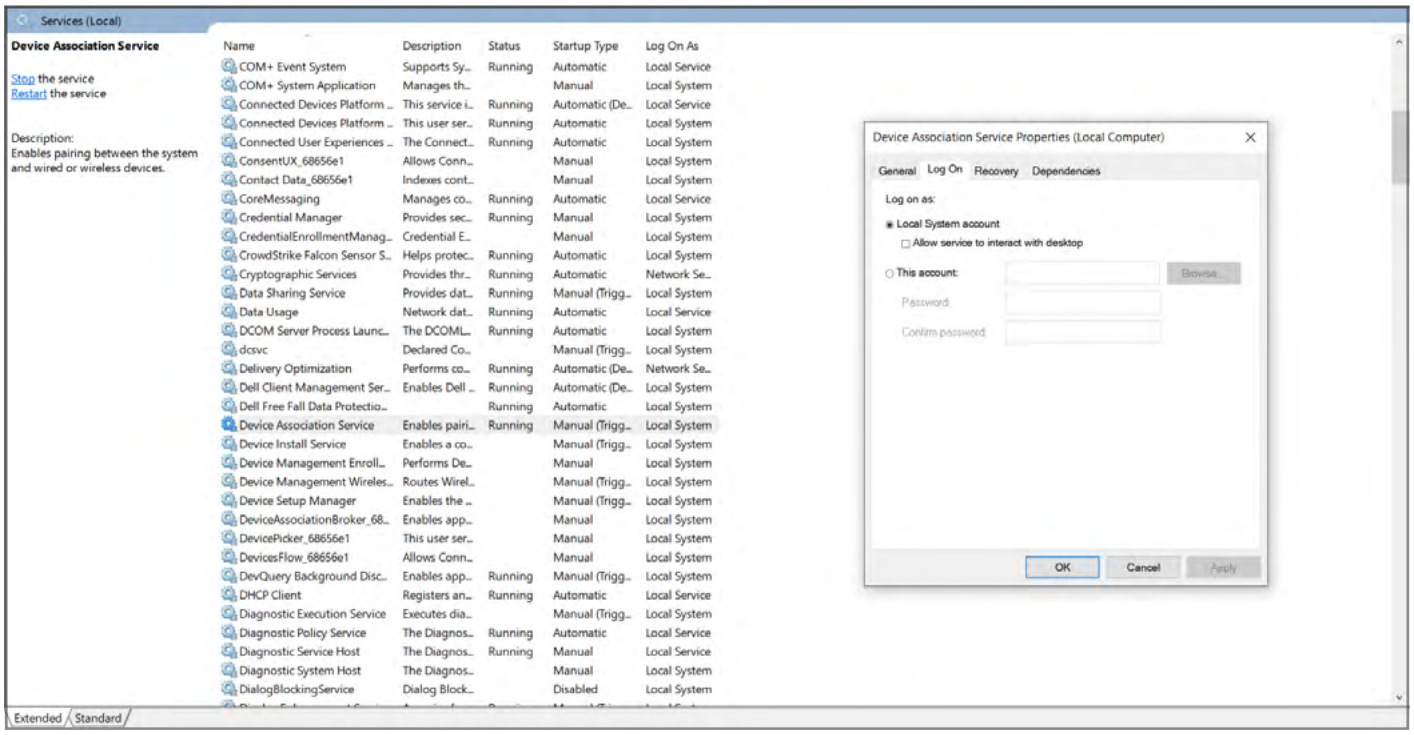
As the description reads, this particular service called Windows Time maintains the date and time synchronization across all servers in the network. This service may require communicating with other machines in the network to provide the accurate time according to the server, it but does not require sharing of credentials. This service is handled by a local service account.

Network Service account



The service Remote Desktop Services authorizes remote desktop connections to and from the respective machine. This is managed by a network service account (refer to the image above) because it requires access to the network and directly works with the computer's credentials.

Local system account



The Device Association Service enables the system to connect to wired and wireless devices. This service works only with the particular machine it is assigned to and needs no network permissions or network access. Therefore, it is assigned to the built-in local system account.

But apart from these built-in service accounts...

Users can create custom Windows service accounts and register them in the Active Directory to assign service to them.

Why though?

This is made possible, because the built-in service accounts are managed by the operating system and by default are tagged to all systems running the Windows OS. External service accounts are created to distribute services selectively to the Windows resources of a network environment.

New service accounts need to be created to add a security context to the services in the Windows OS. This security context refers to the service's permission to access resources, and the user's permission to manage these services.

To simplify, if a new service account is created, it can be used to target specific resources of an organization to perform selective services such as password reset, or other custom actions. Additionally, by creating new service accounts in the Active Directory, an admin can limit the number of users who can manage that particular service account.

Therefore, enterprises favor creating service accounts to assign special privileges to maintain the security needs the service demands due to their crucial functions.

What types of service accounts can be created?

Any created Windows service account is always created in a domain controller, or any machine that has access to the Active Directory. There are two types of service accounts: managed service accounts and domain user accounts. Both of these service accounts can only be attached to individual machines and are more or less similar but also somewhat different.

A domain user account works similar to a local user account, but it is created in a domain controller. It is used to access network services and interact with domain resources for services like file sharing, registry access, and directory services. This is a privileged service account that can be accessed by a human administrator to update passwords periodically.

It is assigned privileges, but only for those particular services this account is attached to. In general terms, a domain user account works the same way as a local human user account, but with privileges that limit its accessibility to services alone.

A managed service account (MSA) is a highly privileged service account and no human user interacts with it. Passwords for these service accounts are updated automatically. It is mandated that the passwords of these service accounts don't expire, because generally these service accounts deal with critical services. There are two types of MSAs: standalone managed service accounts (sMSA) and group managed service accounts (gMSA).

An sMSA is used to automate services across devices in the same server. However, a gMSA is used to perform services in machines across multiple servers, but the machines should belong to a common server farm or they should be distributed by a common load balancer.

Why are service accounts deemed critical and what are privileges in Windows service accounts?

Service accounts in general deal with multiple services that run on various machines at the same time. If one service account fails, it would disrupt all services attached to that account. The damage doesn't stop there. It also scathingly disrupts all service dependent on the services attached to the actual account, resulting in a cascading system failure throughout the organization.

In the case of human user accounts, an admin account has more privileges than a normal user account. According to these varying privileges assigned to them, their levels of access to information within the network will also differ.

Similarly, service accounts also have privileges assigned to them and this privilege assignment defines the service account's access to information within the enterprise network.

Highly privileged service accounts typically handle critical services like establishing remote connections, password vaulting, password reset, etc. Ideally high-level privileges are assigned to service accounts are for services that deal with the security of the system or the network. On the other hand, low-level privileges are assigned to service accounts that deal with distributive services like software updates, file transfers, and patch releases.

Privileged access management (PAM) and service accounts

Any privileged account, especially service accounts need to be secured and managed vigilantly. Single service accounts are widely used to run multiple services at multiple machines throughout an enterprise. A disruption of that account will lead to downtime of multiple applications that the particular service is responsible for performing.

Outdated practices include saving passwords of such service accounts in spreadsheets, text files, and other non-encrypted locations. This leaves room for mass mismanagement of service account credentials which could lead to crippling effects on the network.

Given that a single service account usually delivers multiple services across multiple machines, a disturbed service account will result in widespread disturbances across the network.

To avoid such instances, it is advisable to follow PAM practices that enable organizations to secure service accounts effectively.

In the context of service accounts, some PAM best practices include:

Storing service account credentials in a secure vault:

Discovering service accounts and automatically adding them to a password vault will help the organization to keep track of all functional services and their respective accounts in the vault.

Periodically resetting service account passwords:

Periodic password reset is a mandatory requirement while dealing with service accounts. However, while configuring automatic password reset, never let passwords expire for service accounts since service accounts are critical privileged accounts. Letting a service account password expire is more or less similar to compromising the account since, in both cases, the result is the same: mass failure of services.

Centrally managing service account credentials across the network:

Managing service account credentials centrally, will keep them aware of the number of services tagged to each account, which service accounts run on which domain, when their passwords are due for reset, etc.

These service account management best practices, when incorporated into an enterprise solution are, in effect a PAM solution.

This brings us to our in-house privileged access management solution: **PAM360**.

ManageEngine PAM360 and service account management

PAM360, as an enterprise solution, specializes in service account management best practices and implements these as its gold standard. Using PAM360, organizations can discover, secure, manage, and centrally automate the regulation of privileged service account credentials.

Thanks to ManageEngine's all-around IT solutions suite, PAM360 provides various integration opportunities, crafted to function in an enterprise IT infrastructure and to reduce the complications that surround service account management.

We now arrive at the end of this exploration with the answers to the same questions as when we began.

Service accounts are responsible for holding an IT network together and should be prioritized as the most critical privileged accounts in a network. Service accounts form the crux of the computer's user interface and are the foundation of a network's presence.

ManageEngine

PAM360

www.manageengine.com/pam360