

THYCOTIC PRIVILEGED ACCOUNTS DISCOVERY FOR WINDOWS

krome

What's Next after Discovery?

After you have run the Privileged Accounts Discovery Tool for Windows, you get a document with a management-ready summary of your results and a detailed CSV file of machines and accounts discovered.

If you are like most users, these documents are an awakening—they contain many expired passwords, the names of service accounts that you did not know existed, and the names of administrators who are unknown to you. What now? Now that you've identified these issues, how can you take control of your privileged credentials?

There are some problems you can take care of right now through manual intervention.

Manual steps typically include







- Changing passwords in your most sensitive environments
- Investigating and removing backdoor admin accounts
- Setting a new Windows administrator password in a group policy to ensure former employees no longer know the local administrator password

But it's obvious you need to better control your privileged passwords in the future, or you'll be doing the same manual clean up in a few months.

The Secret Server solution from Thycotic makes it easy for administrators and security teams take control of their privileged accounts. Secret Server from Thycotic goes much further than the free discovery tool because it not only discovers the privileged accounts, it automatically vaults them and applies protection policies around them to keep them under control. Secret Server is a paid-for product that protects and manages the privileged accounts you discovered with the Privileged Accounts Discovery Tool.

 [Run the Discovery Tool](#)

Here are key features in the paid-for Secret Server solution that solve the privileged password vulnerabilities brought to light by the discovery tool:

-  Import discovered privileged accounts to Secret Server automatically
-  Protect the privileged accounts in Secret Server's vault
-  Easily change passwords to meet compliance requirements
-  Easily and completely revoke a user's access through secure automatic password changing
-  Stop unauthorised access. Limit users' access to just the privileged accounts they need
-  Safely use privileged credentials: let admins do their work without even knowing the password they are using; eliminate typing in passwords or saving them in spreadsheets; securely share and open remote sessions with Secret Server.

thycotic 

Your best value to assure privileged account password protection

What are the top 5 benefits you get by upgrading your free Privileged Accounts Discovery for Windows Tool to Secret Server?

1. Securely share and store privileged accounts in a central repository
2. Automatically discover and change privileged account passwords
3. Add additional layers of security against a breach
4. Obtain audit trails, reports, and monitoring to meet compliance
5. Integrate privileged account management with applications and tools already in place



Run the Discovery Tool