Mandiant

CONFIGURE WINDOWS ACCOUNTS

If you want to use non-system accounts during testing, you can by creating Action User Profiles in the Director. Both Local and AD accounts can be used.

- Local Accounts must be created in the Windows environment before their matching Action User Profile can be used.
- AD Accounts do not need to be added to Windows. When you add domain information to the Action User Profile, the Director knows to authenticate against the AD server.

> Running an Action with an AD account that has never logged onto the system may increase the time it takes to run.

> Testing malware controls does not require AD and testing AD policy does not require malware, so using AD Accounts on the Protected Actor is not supported.

Creating Local Windows Accounts

> Instructions provided are for Windows 8, 8.1, and 10. If you are using a different version of Windows, refer to the Microsoft Windows documentation for that version.

1. From the run/search bar (you may need to open the Start menu), type Add User in the run bar, and select Add, edit, or remove other people.
2. Click Add someone else to this PC.
3. Select I don't have this person's sign-in information.
4. Select Add a user without a Microsoft account.
5. Enter the *account information* and *security questions* and then click Next.

> Capture information about the new accounts, including cases used in the username and password, so you can create the account identically in the Director.

6. Click Windows, click the user icon, and then select the new user account.
7. Sign in using that account to create the account profile, setting up Security Questions as required.