KONICA MINOLTA

Dispatcher
Phoenix

User Accounts

This document provides a description and explanation of the security features that are built into the Dispatcher Phoenix software application.

Impersonation

Applications are often configured to use accounts that are granted more privilege than is actually required. Running as an administrator can be a risky practice, leaving your system vulnerable to security risks and exploits. When applications are allowed to run with accounts that are deeply privileged, the system is exposed to compromise.

Following the Windows principle of least privilege, Dispatcher Phoenix addresses these concerns and ensures a more secure environment by using Windows impersonation. This means that the Dispatcher Phoenix application takes on the user's identity after the user is authenticated, instead of running as an administrative service account with broad access to the entire system.

This implementation of user impersonation is a critical and vital differentiating feature of the application, setting it apart from other solutions in the marketplace today. Impersonation, known as one of the most useful mechanisms in Windows security, allows Dispatcher Phoenix to avoid granting one account unlimited access to folders, which can open up major security vulnerabilities throughout the system. For example, in Dispatcher Phoenix, folders are accessed as the logged-in user, not as an administrative service account that has read/write access to all network folders. By impersonating the Active Directory user, Dispatcher Phoenix ensures that ONE user does not have access to ALL folders.

User Accounts

When Dispatcher Phoenix is installed, only one user account (./***conopsd***) is created to provide the bare minimum number of privileges required to make workflows run. In addition, a virtual user account (***blox-log***) is created to capture/create the workflow logs when a workflow is running.

- **./conopsd**
  This user account is responsible for making sure that the Workflow Services have the ability to start the workflow processes necessary to process documents in a workflow. Although it provides the level of access necessary to run tasks, the ./conopsd user account has actually less privileges than the System Account has. With this account, you can see exactly what the Dispatcher Phoenix Workflow Services and Worker Services are doing and also adjust privileges as necessary so that conopsd only has those privileges required to perform the required tasks. The conopsd account is not configured to be able to log into the PC and cannot create other user accounts.

- **blox-log**
  blox-log is not a security group and only exists when the KMBS Logging Service is running. In line with Microsoft's Best Practices, this service can be monitored independently of the other services that are running under the System Account.