

MessageOps Password Synchronization



www.MessageOps.com

info@messageops.com

Introduction

MessageOps Password Synchronization allows organizations to synchronize passwords from their local Active Directory to Microsoft Online. The MessageOps Password Synchronization consists of 3 major parts:

- Password Filter
- Client Service
- Server Service

The Password Filter captures the password within the Local Security Authority (LSA) on the Domain Controllers. The Client Service sends the password request to the Server Service. The Server Service accepts password change requests and sets the password within Microsoft Online.

The Password Filter

The Password Filter is a DLL that is installed with the Client Service on each Domain Controller in a Domain. Its job is to intercept user password changes. When it intercepts the username and password they are in clear text. It encrypts the username and password in a file which is then processed by the Client Service.

The Client Service

The Client Service is responsible for processing the password change files generated by the Password Filter. As mentioned above, it must be installed on every Domain Controller in the environment. The first thing the Client Service does is decrypt the username and password file. It then evaluates the username to see if it matches an LDAP Filter. The LDAP Filter is configurable through the Password Client Admin Interface, shown below.

The screenshot shows a window titled "Password Client Admin Interface" with a menu bar containing "Log", "Service", "Server", "Cryptography", and "About". The "Server" menu item is selected. The window is divided into two main sections:

- Password Server:** Contains two input fields: "Server IP Address/Hostname" with the value "dirsync" and "Server Port" with the value "13746".
- LDAP Server:** Contains two input fields: "Root Query" with the value "LDAP://localhost" and "Filter" with the value "(&{samAccountName={0}})(objectCategory=person)(objectClass=user)". Below the filter field, a note states: "The token {0} will be replaced with the samAccountName".

In the example above you can see the filter would apply to all user objects. Password resets for Computer objects would be discarded by the client (since they don't match the filter), and are not forwarded to the Password Server. Using the LDAP filter you can define a subset of users whose passwords you want to synchronize. If the username matches the LDAP filter, the Password Client

establishes an encrypted connection to the Password Server, which is also configurable through the Password Client Admin Interface, shown above. Once the connection is established to the Password Server the Password Client waits for a response from the Password Server, before deleting the password file and moving onto the next password change file.

The Server Service

The Server Service is responsible for accepting Password Client connections and setting the passwords within Microsoft Online. One Password Server can handle requests for multiple Password Clients. When a request comes in from a Password Client it launches a new PowerShell instance to perform the password reset. The results of the PowerShell command are parsed and returned to the Password Client.

Requirements

- The Client Service and Filter should be installed on all domain controllers.
 - Requirements:
 - .Net 3.5
 - Windows 2003 or higher
 - X86 and X64 versions are supported
- The Server Service is installed on a single server in an organization and all Password Clients will report to the single Password Server.
 - Requirements:
 - Microsoft Online Migration Tools
 - .Net 3.5
- Microsoft Online Directory Synchronization must be running in the environment.

Questions?

If you have questions, please contact MessageOps at info@messageops.com.