

**Password Expiration Scanner Guide**

Version 1.0

September 2014

Table of Contents

[Password Expiration Scanner 3](#_Toc399408954)

[Configuring SERI AD Image 3](#_Toc399408955)

[Task Definition Properties 6](#_Toc399408956)

[Notes & Possible Issues 7](#_Toc399408957)

# Password Expiration Scanner

A common use-case is to have users notified of upcoming password expirations. This task allows for the scheduling and configuration of notifying users that their password is about to expire. The PasswordScanner task will query Active Directory for the *MaxPwdAge*, then another query for users whose *pwdLastSet* is between a configured range. This method was chosen since checking every user in IdentityIQ can be costly, storing the pwdLastSet in IdentityIQ is not ideal, and LDAP is efficient at queries.

# Configuring SERI AD Image

The SERI Active Directory Image has a default MaxPasswordAge of 42 days. All of the current user's password was last set greater than 42 days ago, so all users have expired passwords.

To configure the MaxPwdAge:

Open **Group Policy Management** under Administrative Tools:

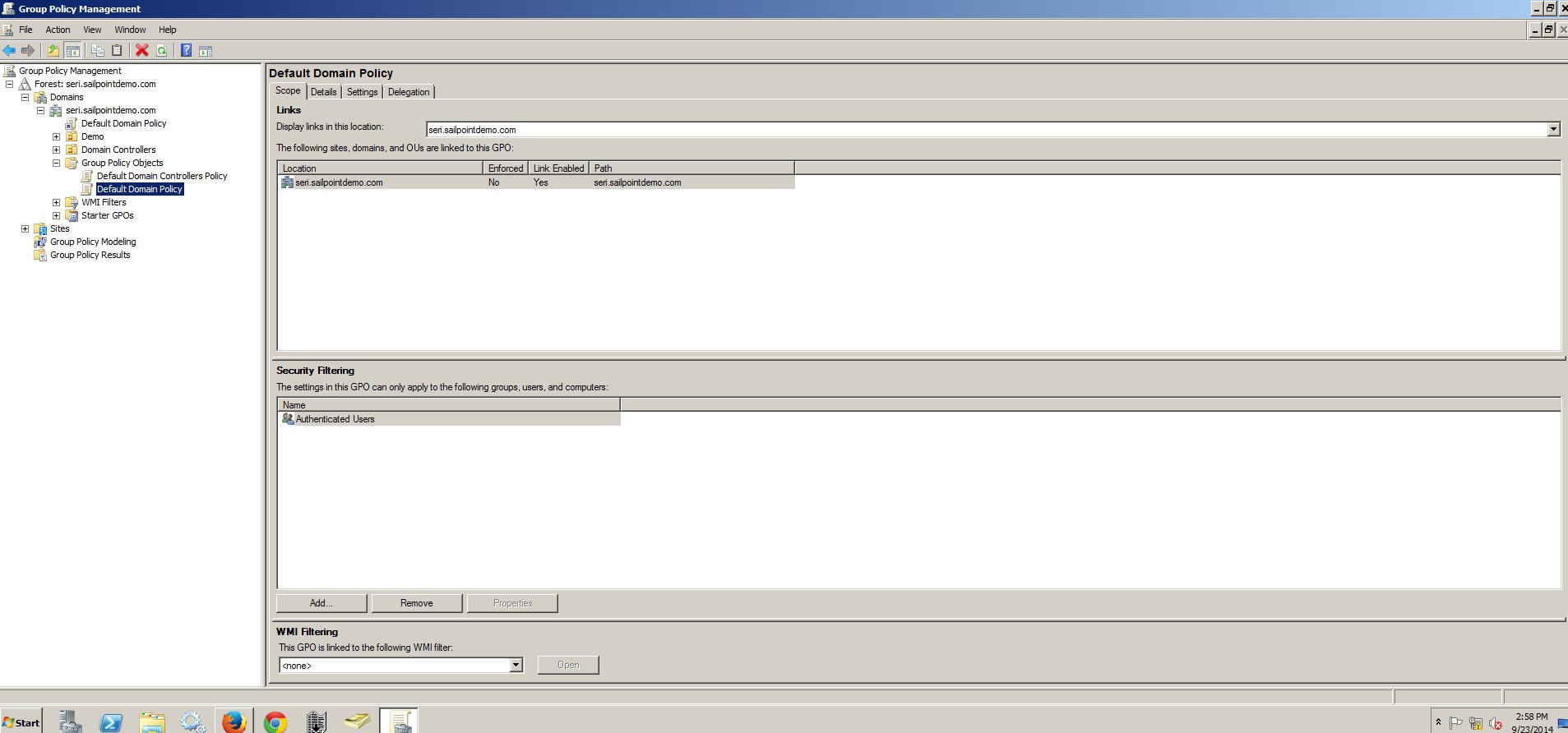


Figure : Group Policy Management

1. Edit the *Default Domain*:
   * Forest: seri.sailpointdemo.com -> Domains -> seri.sailpointdemo.com -> Group Policy Objects

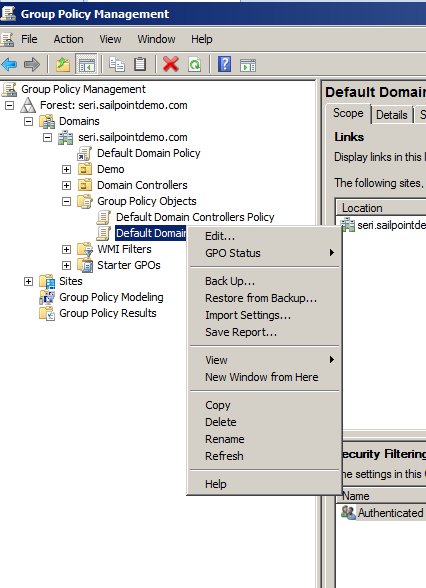


Figure : Default Domain

1. Select the Password Policy:
   * Computer Configuration -> Policies -> Windows Settings -> Security Settings -> Account Policies -> Password Policy

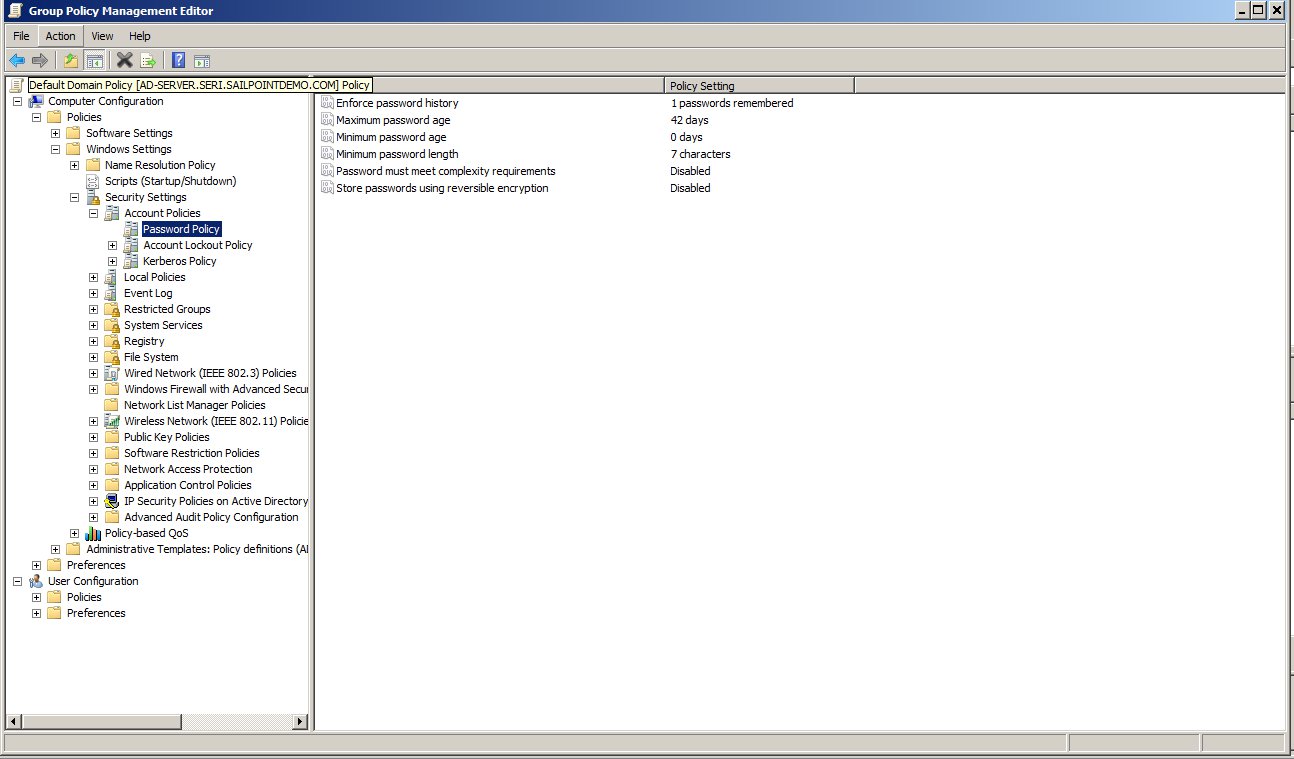
****

Figure : Password Policy

1. Double Click the Maximum Password Age and select a value:

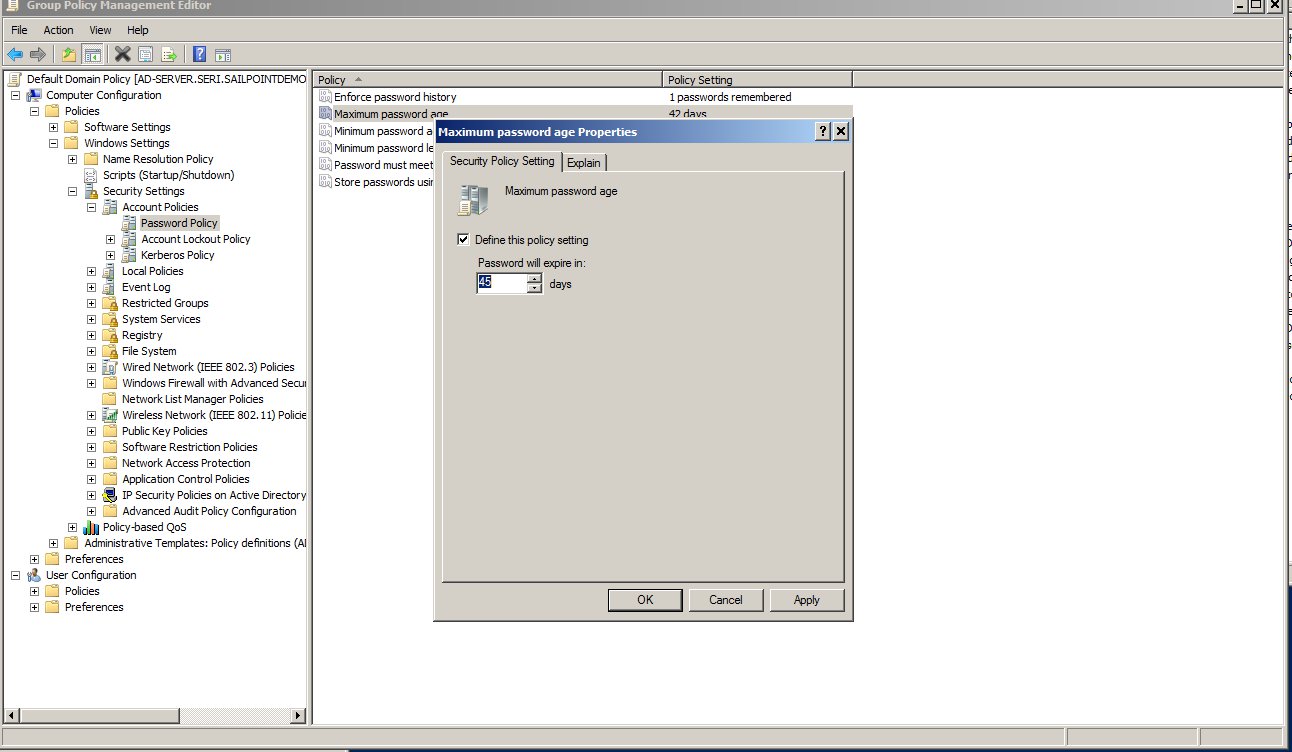


Figure : MaxPwdAge

1. Wait one minute
2. A powershell script is included to check these values. Maxpwdage.ps1
3. Change a user's password
4. Run the Scanner with at least one value in the CSV range to be MaxPwdAge -1

NOTE: For day ranges the PasswordScanner uses the convention of 41 days, 0 hours, 0 minutes, 0 seconds to 41 days, 23 hours, 59 minutes, 59 seconds to be a range of 43 days. This means if the MaxPwdAge is set to 42 days, then when the user's password is set they will be "caught" in the 41 day scan if run within the next 24 hours. This also means that to catch users whose password will expire the day of the scan ( < 24 hours) a value of 0 is used.

# Task Definition Properties

* Expiring Email Template – Set to "**Password Expiration Notification-HTML**". TaskDefinitions don't easily allow a default value when dealing with sailpoint objects.
* Expired Email Template – Set to "**Password Expired Notification-HTML**"
* Application to Scan for Expiring Passwords – Set to "**Active Directory**" TaskDefinitions don't seem to allow filters. Currently ActiveDirectory is the only supported connector type
* Is OpenDJ – Currently does nothing, will be used when SunONE Directory is supported
* CSV List of Range – Set to a CSV range of date (e.g. 15,10,5,1).
* Include users whose account never expires – Not implemented yet
* Override User – PasswordScanner will connect with the credentials configured in the Active Directory app definition, if this needs to be overridden with a different user, then enter here.
* Override Password - PasswordScanner will connect with the configured settings of the Active Directory app definition, if this needs to be overridden with a different searchDN, then enter here.
* Override SearchBase - PasswordScanner will connect with the credentials configured in the Active Directory app definition, if this needs to be overridden with a different user, then enter here.
* Cn=Domain base for AD – Set this to the Root DN for AD. (e.g. dc=seri,dc=sailpointdemo,dc=com)
* Enable Test Mode – If set, then no emails are sent
* Notify Users of already expired passwords – Separate scan for users with expired passwords.

# Notes & Possible Issues

* Active Directory Time is the number of 100 nanoseconds since Jan 1, 1601
* Java Time is milleseconds since Jan 1, 1970
* MaxPwdAge is stored as a negative value. For example, 45 days is stored as -38880000000000
* Helpful Utility for Time Conversion : <http://www.epochconverter.com/epoch/ldap-timestamp.php>
* Does not currently support searchDNs. If the application definition has more than one searchDN defined, use the Override SearchBase
* If the user does not have permission to search the root DN (dc=seri,dc=sailpointdemo,dc=com) this will fail