Enrollment best practices

Purpose

Provide best practices for policy configuration in order to simplify the enrollment process for end users.

Introduction

From version 8.9 of the Specops Authentication engine, the enrollment process for end users has been simplified. Instead of being presented with an overview of all the associated applications and having to enroll separately for each, users will now be directed immediately to the enrollment process itself (gathering of stars). Correctly configured policies across services/applications allow users to enroll for all applications by authenticating for shared identity services only.

While the number and configuration of individual policies has now been obscured from end users, it is important for administrators to configure policies in such a way that users are required to enroll with the minimum number of ID services. This document briefly describes what such a configuration can look like.

Description of process

The order in which ID services are presented during the enrollment process is determined by the configured weight of the ID service itself, as well as the weight of the policy it is a part of.

1. Enrollment process will first cycle through all **required unenrolled ID services**.
2. Next, the **most complex policy** will be presented. This is the policy with the most unenrolled stars.
3. In that policy, the **most complex ID service** will be presented first, i.e. the one with the most stars, followed by progressively less complex ones, if they are present.
4. If the policies for the sources/applications have been configured with identical ID services, the process will terminate there (unless the user wishes to add more stars). Otherwise, once the policy is completed, the process will move on to the next most complex policy and so forth.

Best practice

In order to make the enrollment process as simple as possible for all users, regardless of which applications are affected, it is advised that the **same ID services are configured for all applications for user groups sharing a policy**. While it is still possible to configure different sets of identity services for different applications, doing so means that the enrollment process will take longer, since users will have to fulfill all stars in order to complete the process.

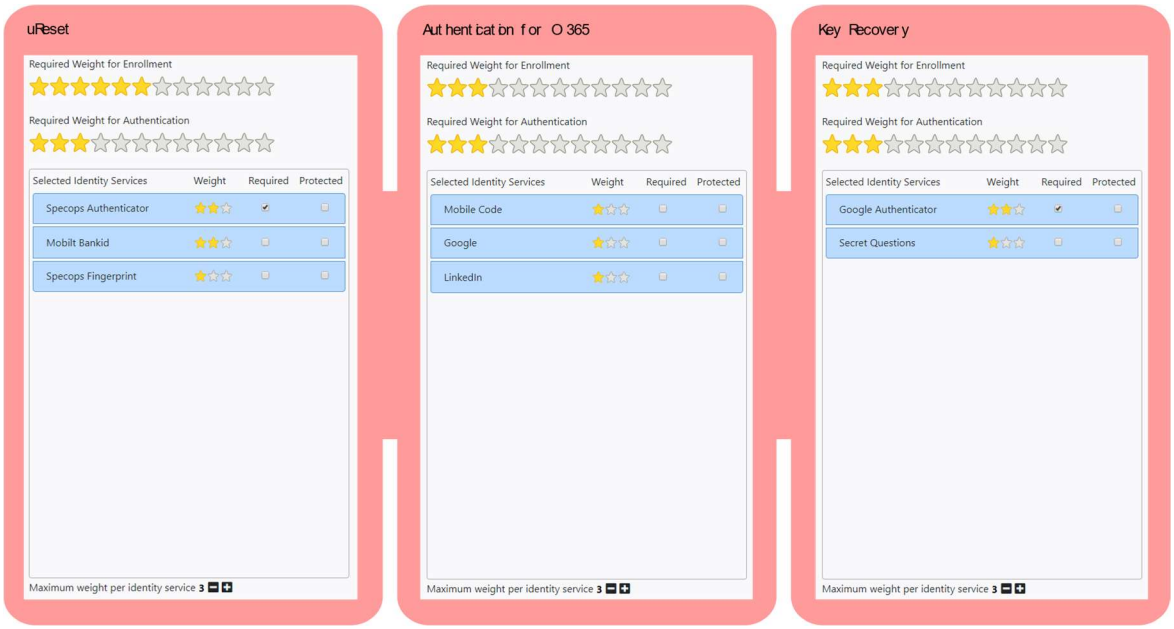
Examples

The examples given here show somewhat simplified configurations to illustrate how differences in policy configuration can affect end user experience.

Example 1

Three applications, different ID services in each policy

Minimum enrollment: 8 ID services

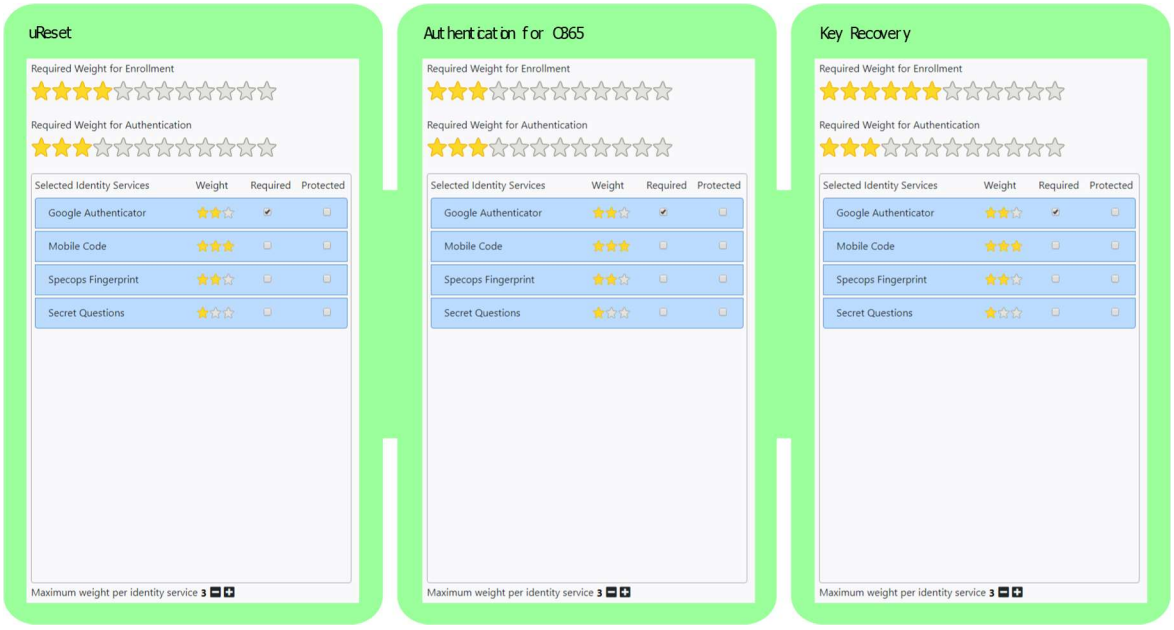


In the above example, the user would have to enroll with **all eight** ID services since they are different for all applications. The enrollment process would start with Specops Authenticator, followed by Google Authenticator (the two required services), followed by a choice of Mobile Bank ID and Specops Fingerprint (both of which have to be enrolled to obtain the required number of stars). The process would then move on to the less complex policies, presenting Google, LinkedIn, and Secret Questions.

Example 2

Three applications, identical policies for all three

Minimum enrollment: 3 ID services



In this example, the user can enroll with a minimum of **three ID services** (with optional extra stars) to complete the enrollment. The enrollment process would start with Google Authenticator (required), then present three options: Mobile Code, Specops Fingerprint and Secret Questions (from the Key Recovery policy since that is the most complex of the three). The user can then choose which

services to enroll with; the minimum being Mobile Code and one other ID service. Once all star requirements have been met, the user can gather additional stars by enrolling with the remaining ID service as well.

Re-Enrollment

When users enroll for the first time, they will have to identify themselves by providing their Windows password. Subsequent changes to enrollment (re-enrollment) will require identification with one previously used identity service in addition to their Windows password, if the security mode is set to Medium or High.

There are three security modes available to administrators: Low security, Medium security, and High security. These security modes reflect the relative strength of the policies configured, and determine in part which identity services the user needs to re-enroll with (whenever users need to change their enrollment).

Low security
Users are only required to provide their Windows password for identification.

Medium security
Upon re-enrollment, users are required to identify with one previously used identity service in addition to their Windows password.

High security
Upon re-enrollment, users are required to identify with one previously used strong identity service, or two weak ones (in case they have not enrolled with any strong identity services), in addition to their Windows password. Weak identity services, such as security questions, will not be presented to the user as an option, unless they have enrolled only with weak identity services.

Note: the low or medium modes are set automatically, depending on the policy configurations. High security mode has to be enabled by administrators in order to enforce re-enrollment with strong identity services.

Identity Services Selection Guide

Not all identity services are created equal. To help you select the best fit for your organization, we have created the matrix below, with the following criteria:

- The MFA factor the identity service addresses: something you know, something you are, some- thing you have.
- The enrollment flexibility: pre-enrollment and/or administrator enrollment using existing Active Directory data.
- Mobile dependency

When selecting an identity service, it is important to also evaluate the user experience, including how familiar it is to the user.

Identity Service	Something you know	Something you have	Something you are	Pre/ Admin Enrollment	Mobile phone based	Active Directory Data
Specops Fingerprint	●	●	●		●	
Mobile Code	●	●		●	●	Mobile number

Identity Service	Something you know	Something you have	Something you are	Pre/ Admin Enrollment	Mobile phone based	Active Directory Data
Symantec VIP	●	●		●	One of the delivery methods	Attribute where Symantec user ID is stored
Duo Security	●	●		●	●	samAccountName
Manager Identification	●	●		●		Manager
SITHS		●		●		userPrincipalName
Mobile Bank ID	●	●		●	●	Sub object
Security Questions	●			●		Varies by question
Specops Authenticator	●	●			●	
Google Authenticator	●	●			●	
Microsoft Authenticator	●	●			●	
LinkedIn	●	☆				
Gmail	●	☆				
Microsoft Live	●	☆				
Facebook	●	☆				
Twitter	●	☆				
Flickr	●	☆				
GitHub	●	☆				
AOL	●	☆				
Yahoo	●	☆				

☆ Social identity services that allow a second factor, primarily mobile verification code via SMS. Microsoft Live, Gmail and GitHub also support One Time Password (OTP) apps.