With the increasing use of cloud services, bring your own device policies and the blurring of enterprise boundaries the risk landscape faced by IT Security has never been so diverse.

To help enterprises manage this environment Swivel has developed a range of risk based authentication capabilities. These capabilities ensure enterprises can address their current and evolving authentication strategy for securing access to a range of resources using a single authentication platform.

User experience is optimized without compromising security and enterprises are not limited to a one size fits all approach.

We don’t make the rules; you do, so your implementation will be unique to your specific needs.

**Policy Engine**

The policy engine allows you to determine what form of authentication is appropriate for any one authentication. The policy engine makes the decision based on a number of factors determined by you as being significant risk factors. These factors may include:

• Who the user is
• What service the user is trying to access
• What IP address is the user is accessing from
• The time of access
• The device the user is using
• When the user last authenticated

The policy engine allocates the user points based on these factors. These points are then used to determine what form of authentication is appropriate for this access required. This may take the form of

• Username and Password
• Swivel Strong Authentication
• Swivel Two-Factor authentication

**Authentication Portal**

All authentications are rooted through a single login point no matter what applications; be it in the cloud or on premise.
Single-Sign-On

A special case for the policy engine is that the user is not required to perform any authentication. This is where the user is allocated points for having recently authenticated to a different service via the authentication portal within the same browser session. In this case the user is automatically granted access, which means the user can enjoy single-sign-on.

Flexibility

The points scoring system is completely flexible. You can decide what points are allocated to each factor within the policy engine meaning each installation can be tailored to the unique requirements of your organization.

Extensibility

The policy engine is extendable and new policies can added easily added at any time.

Technical Specs

<table>
<thead>
<tr>
<th>Platform</th>
<th>Specifications</th>
</tr>
</thead>
</table>
| Authentication Portal Compatibility | Cloud Services (SAML)  
Web Applications (via Swivel .Net Plug-in) |
| User Policy                     | Based on Group Membership                           |
| IP Address Policy               | Based on ‘trusted’ IP address range                 |
| Device Policy                   | Based on X.509 Certificates                         |
| Location*                       | Based on GeoIP                                      |
| Know IP*                        | User has authenticated from this IP address before   |
| Time of Day                     | Safe hours and unsafe hours                         |

*Roadmap