

Login Security Policy Extension

draft-gould-regex-login-security-policy

James F. Gould

jgould@verisign.com

IETF-103 REGEXT Working Group

Introduction

- Login Security Policy Extension is the first system-level policy extension of the Registry Mapping (draft-gould-carney-regext-registry) for the Login Security Extension (draft-gould-regext-login-security)
 - Included in response to <registry:system> Registry Info Command
- Defines the MAYs, SHOULDs, and supported options of draft-gould-regext-login-security (<https://tools.ietf.org/html/draft-gould-regext-login-security>)
- <https://tools.ietf.org/html/draft-gould-regext-login-security-policy>

Login Security Policy Information

- Login password format policy
 - Uses Perl-compatible Regular Expression (PCRE) syntax for format
 - Provides optional human-readable description for format policy
- User agent support boolean
 - Boolean with default of "0" (or "false") indicates that the server processes the client user agent information
- Policies for supported typed security events
 - Levels that may be returned ("warning", "error")
 - Expiry date boolean indicating whether the event includes an expiry date with:
 - Warning period (duration)
 - Expiry period (duration)
 - Indicate error that will occur at expiry ("connect", "login", "none")
 - Threshold for a "stat" security event
 - Period (duration) for a "stat" security event

Login Security Policy Example

```
<loginSecPolicy:system>
```

```
<loginSecPolicy:pw>
```

```
<loginSecPolicy:expression>
```

```
(?=\.*\d)
```

```
(?=\.*[a-zA-Z])
```

```
(?=\.*[\x21-\x2F\x3A-\x40\x5B-\x60\x7B-\x7E])
```

```
(?!^\s+)
```

```
(?!.*\s+$)
```

```
(?!.*\s{2,})
```

```
^\[\x20-\x7e]{16,128}$
```

```
</loginSecPolicy:expression>
```

```
<loginSecPolicy:description>
```

16 to 128 printable characters (alphanumeric, space, and special characters) with at least one number, letter, and special character, with no leading or trailing whitespace, and with no consecutive spaces.

```
</loginSecPolicy:description>
```

```
</loginSecPolicy:pw>
```

```
...
```

Login Security Policy Example

...

```
<loginSecPolicy:userAgentSupport>true</loginSecPolicy:userAgentSupport>
```

```
<loginSecPolicy:event type="password">
```

```
  <loginSecPolicy:level>warning</loginSecPolicy:level>
```

```
  <loginSecPolicy:level>error</loginSecPolicy:level>
```

```
  <loginSecPolicy:exDate>true</loginSecPolicy:exDate>
```

```
  <loginSecPolicy:exPeriod>P90D</loginSecPolicy:exPeriod>
```

```
  <loginSecPolicy:warningPeriod>P15D</loginSecPolicy:warningPeriod>
```

```
  <loginSecPolicy:exError>login</loginSecPolicy:exError>
```

```
</loginSecPolicy:event>
```

```
<loginSecPolicy:event type="certificate">
```

```
  <loginSecPolicy:level>warning</loginSecPolicy:level>
```

```
  <loginSecPolicy:level>error</loginSecPolicy:level>
```

```
  <loginSecPolicy:exDate>true</loginSecPolicy:exDate>
```

```
  <loginSecPolicy:warningPeriod>P15D</loginSecPolicy:warningPeriod>
```

```
  <loginSecPolicy:exError>connect</loginSecPolicy:exError>
```

```
</loginSecPolicy:event>
```

...

Login Security Policy Example

...

```
<loginSecPolicy:event type="cipher">  
  <loginSecPolicy:level>warning</loginSecPolicy:level>  
  <loginSecPolicy:exDate>>false</loginSecPolicy:exDate>  
</loginSecPolicy:event>  
<loginSecPolicy:event type="tlsProtocol">  
  <loginSecPolicy:level>warning</loginSecPolicy:level>  
  <loginSecPolicy:exDate>>false</loginSecPolicy:exDate>  
</loginSecPolicy:event>
```

...

Login Security Policy Example

...

```
<loginSecPolicy:event type="stat" name="failedLogins">
  <loginSecPolicy:level>warning</loginSecPolicy:level>
  <loginSecPolicy:exDate>>false</loginSecPolicy:exDate>
  <loginSecPolicy:threshold>100</loginSecPolicy:threshold>
  <loginSecPolicy:period>P1D</loginSecPolicy:period>
</loginSecPolicy:event>
<loginSecPolicy:event type="custom"
  name="myCustomEvent">
  <loginSecPolicy:level>warning</loginSecPolicy:level>
  <loginSecPolicy:exDate>>false</loginSecPolicy:exDate>
</loginSecPolicy:event>
</loginSecPolicy:system>
```

Conclusion

- Login Security Policy Extension
 - First example of a system-level Registry Mapping policy extension
 - Defines the server policies associated with the Login Security Extension
 - Login password format policy
 - User agent support policy
 - Security event policies
- Please review the draft and provide feedback on the mailing list