Privileged Identity Application Launch Supported Web Browsers

The Privileged Identity Application Launch web application has been tested with the following browsers:

- Internet Explorer 9, 10, and 11
- Microsoft Edge
- Firefox
- Google Chrome
- Safari
- Konqueror
- Opera

Following are *known* caveats when working with these browsers:

Microsoft Internet Explorer

- On Server operating systems with Internet Explorer Enhanced Security Mode (IE ESC) enabled, the web application will fail to render or function properly.
- CORS support is only available to IE v10 and later. To enable CORS support, you *may* need to set the following IE option:
    - **Internet Options > Security tab**, for the correct zone click on **Custom Level** button. Find the **Miscellaneous** section and enable: **Access data sources across domains**.

Microsoft Edge

- ActiveX RDP control for launching into RDP sessions (not app launcher sessions), cannot function with this browser. Edge does not support ActiveX controls.
- *Click-Once* extension required to support application launching. Edge does not support Click-Once.

Google Chrome

- *Click-Once* extension required to support application launching. This is currently only supported by Chrome on Windows for application launching.
- *IE Tab* extension required to support the ActiveX RDP control for launching into RDP sessions (not app launcher sessions). This is currently only supported by Chrome on Windows RDP session launching.
- As of Chrome 58, SSL certificates that do not include a properly formatted SAN (Subject Alternative Name) value will be shown as insecure sites. This in turn will cause the user extra prompts and likely break access to the web service which is required for web application functionality. To use Google Chrome, ensure you have a valid Subject Alternative name value added into your certificate.
- Integrated Windows Authentication can be supported by Chrome for scenarios where cross origins requests (CORS) must be used by launching chrome with the following flags (note Chrome will show a security warning about this):
    - **--disable-web-security --user-data-dir=SOMEDIRECTORY**

Mozilla Firefox

- *Click-Once* extension required to support application launching. This is currently only supported by Firefox on Windows for application launching.
- ActiveX RDP control for launching into RDP sessions (not app launcher sessions) is not supported in Firefox.
- Integrated Windows Authentication is available for browsers running on Windows operating systems that are joined to a trusted domain provided the following configurations are made to the user's browser profile:
- For Kerberos authentication, enable **network.negotiate-auth.trusted-uris** and define the target domain name. For example, if the domain DNS name is *lsds.int*, enter it as *.lsds.int*; notice the leading dot.
- Define if Kerberos ticket passing is required: **network.negotiate.auth.delegation-uris**.
- Define if NTLM authentication: **network.automatic-ntlm-auth.trusted-uris**.
- Firefox plans to drop support for Java in 2018.
- CORS support is only available for Firefox v50 and later.

Apple Safari

- BeyondTrust is unaware of any extensions which can enable Click-Once support, thus application launching is not supported with this browser.
- ActiveX RDP control for launching into RDP sessions (not app launcher sessions) is not supported in Safari.
- CORS support is only available for Safari v9 and later.

Konquerer

- BeyondTrust is unaware of any extensions which can enable Click-Once support, thus application launching is not supported with this browser.
- ActiveX RDP control for launching into RDP sessions (not app launcher sessions) is not supported in Konquerer.

Opera

- BeyondTrust is unaware of any extensions which can enable Click-Once support, thus application launching is not supported with this browser.
- ActiveX RDP control for launching into RDP sessions (not app launcher sessions) is not supported in Opera.
- CORS support is only available for Opera v41 and later.