

Q & A from TriCipher's myOneLogin VPN Authentication Webinar, 7-24-08

Q. This looks great for remote access for access to the company's internal network. However, has myOneLogin been used for customer financial product MFA (i.e. online banking, brokerage, etc)?

A. myOneLogin is built on the TriCipher Armored Credential System that has been deployed by many banks and Financial Service providers for protecting consumer facing financial web applications.

-40 Customers – 1000's of Banks - Millions of Users:

-Metavante: over 1,000,000 credentials issued

-FNFI: over 750,000 credentials

-Bank of NY/Mellon: multiple apps accessing auth infrastructure

Q. What steps would I need to go through to get the browser certificate onto my machine?

A. Creation and placement of the browser certificate is handled entirely by the myOneLogin Self Enrolment process.

1. The User enters their user name that has been provided by the SSL VPN administrator.
2. The user enters their password and confirms the password. Once successfully validated against the VPN, the myOneLogin self enrollment continues.
3. The user accepts the TriCipher End-User License Agreement.
4. The user selects a Confidence Image to be displayed to the user during future logins to assure that the user is really connecting to myOneLogin for authentication.
5. The user creates a Welcome Message to be displayed along with the image during future logins to assure that the user is really connecting to myOneLogin for authentication.
6. The user configures answers for Security Questions used for secondary authentications and establishment of a second factor on addition computers that the user connects from.

7. The user registers a second factor on the machine the user is currently connected with. The second factor can be a cookie or browser certificate. The administrator can make this selectable by the user or enforced by policy.

8. The user is granted access having used strong authentication. This access was granted by the session posting a SAML assertion and authorizations allowed for the specific user as configured in the Juniper SSL VPN.

Q. Can we tunnel directly to specific apps that are protected by Juniper or does getting into Juniper mean I have to then navigate and provide credentials to each app I have access to?

A. For web based applications that support SAML, no addition logins would be required once that application is configured to trust the SAML assertion from myOneLogin. For those wishing to add SAML support to their existing web apps they control, we offer freely either the myOneLogin SAML Consumer Module or the myOneLogin SAML Consumer Service.

Q. How does this work with Mobile devices?

A. myOneLogin should work with mobile devices that offer web browsing with cookie or certificate storage. To date TriCipher has not done any official testing of any mobile platforms.

Q. Does this only work with Juniper or do you support other VPN vendors?

A. myOneLogin can support most any SSL VPN that can use SAML, such as Microsoft IAG, or Forms Based authentication.

Q. How do you prevent the browser cookie from being used by another device?

A. The browser cookie is the second factor. For the user to authenticate they must also know the first factor, the username and password. Multiple devices can be registered by the user by answering security questions that were configured during enrollment. Optionally, administrators can limit the number of devices a user is allowed to register.

Q. Does this protect us against keylogging?

A. No. The best protection to date against keylogging is still prevention and detection.

Q. Do you have specific administrative guides for configuring Juniper SAML

A. Yes, TriCipher supplies full documentation as to what is required to configure the Juniper VPN to receive myOneLogin SAML assertions.

Q. Will you make a copy of these presentation slides available?

A. Yes, these were sent out to all participants and the recorded webinar is available on the website

Q. Our company currently uses Juniper SSL 2 VPN. One challenge we have is that our Desktop Team that provides remote support Unable to switch user credentials following a logoff - even when 2nd user acct has VPN cert pre-installed. What about your product?

A. This would not be a problem with myOneLogin.

Q. How does MOL protect credentials that are used to access SaaS sites to ensure that the MOL can't become a target for identity compromise?

A. See Next Question.

Q. What certifications do you have for your hosted service? How do I know my passwords won't be intercepted on your site?

A. myOneLogin uses the proven TriCipher Armored Credential System (TACS) to provide strong authentication for the service. TACS powers the web security for millions of financial and healthcare users. TACS has a U.S. government Federal Information Processing Standard (FIPS) 140-2 Level 2 rating.

FIPS 140-2 is a US government standard that provides a benchmark for implementing cryptographic software. It offers best practices for implementing cryptographic algorithms, handling key material and data buffers, and working with the operating system. FIPS 140 validation is an additional proof performed by third party that demonstrates that a security software implementation meets the highest standards.

Data Security

myOneLogin provides end-to-end strong security from the user's browser all the way to the back-end data stored in myOneLogin.

- At the browser level, browsers use strong authentication to access the myOneLogin service.
- Data is secured in transmission using SSL (HTTPS) protocol or mutual SSL.
- At the back-end, data is protected with database encryption and roles-based access control. myOneLogin administrators cannot view or use the encrypted user information.

A Secure Application Platform

myOneLogin uses a multi-tenant architecture to deliver a robust and secure solution to all its customers. In a multi-tenant architecture, all customers use the same architecture, schema and security from a single myOneLogin service.

myOneLogin leverages TACS to lock down each customer in their own “realm.” Using strong security and role-based access, customers only have access to information in their own realm. This ensures a truly secure multi-tenant architecture.

Data Center Security

The myOneLogin service is hosted in a third-party SAS 70 Type II-certified data center that employs advanced security and protection technologies, including:

- Physical security, including around-the-clock guards and biometric access control.
- A certified staff providing around-the-clock support and real-time monitoring.
- Fully-redundant power systems
- Fire suppression and environmental monitoring

Q. Our current TriCipher MFA solution requires our online banking customers register each device on each product. If they have 3 products and 3 devices, they must register 9 times... will myOneLogin correct this and allow just one registration mul prd/devs?

A. myOneLogin provides not only Strong Authentication but also Single Sign On and Identity Federation. This mean through one strong authentication users will then have sign click access to applications allowed by your administrator.

Q. Why would I select a cookie instead of a cert for second factor?

A. Cookie as a second factor provides for a slightly easier user experience where browser certificate provides stronger security by protecting against Man In The Middle attacks.

Q. Please explain what you mean specifically when you say myOneLogin being used for Juniper SSL VPN's. Does myOneLogin work w/other networks?

A. myOneLogin can be used as Strong Authentication as a Service only to the SSL VPN to create a seamless user experience for connecting to VPN services. However, myOneLogin offers additional capabilities for being a Single Sign On portal for all of the web apps you and your users access whether they are external or internal.

Q. Can we download the presentation or have a copy mailed to us?

A. The presentation was sent out to all participants and is also available by request. Email securevpn@tricipher.com or visit our website at www.myonelogin.com to see the recorded webinar.

Q. What OS and browser platforms are supported for both cookie and certificate second factor of authentication

A. Any browser the can accept cookies or store certificates. TriCipher has done extensive testing with Internet Explorer, Firefox, and Safari.

Q. How are deep links to our application handled with this solution? Do I need to always start at myOneLogin or can we redirect back to you and then have you authenticate and redirect back?

A. When connecting to deep links that go to a web application that supports SAML, the user's session will validated. If the authenticated session is still active, the user is allowed in. If the user's session has expired the user would authenticate and be redirected back to the application with a SAML assertion.