LiveAction

Enabling PIV/CAC Authentication in LiveWire

Quick Guide

ver. 24.3.0a

Introduction

LiveWire supports the use of PIV or CAC cards (PIV/CAC) rather than passwords to authenticate users. This document describes the manual steps necessary to enable the feature in LiveWire.

Note Active Directory may be used as the centralized database of user accounts and is the preferred method for managing access to LiveWire. It allows administrators to easily enable or disable login to all LiveWires with a single operation on the Active Directory server and typically works with the UPN in a transparent manner. Please follow the instructions in the *LiveWire User Guide* for setting up LiveWire to integrate with Active Directory.

About PIV/CAC Authentication

PIV/CAC login is supported via TLS's client authentication option as described in the TLS standard. This option allows authentication using a private key and digital certificate. The PIV/CAC card contains the private key and certificate and performs the cryptographic operations necessary to verify the holder's identity.

Users are generally familiar with the idea of making secure connections to websites, such as a banking site, from their browsers. Such secure connections are often indicated by a "lock" icon or other indicator in the user's browser that a secure, trusted connection has been made and if the connection fails, they are warned that the connection is not secure and discouraged from continuing. In this scenario, the website sends the user's browser a digital certificate containing its identity (e.g., "www.bankofamerica.com") and its public key. If the certificate appears valid, the user's browser will use the information it contains to cryptographically challenge the website to prove it is in possession of the corresponding private key. If the website is successful, a secure connection is made. The user typically authenticates their identity by entering their name and a password into a page on the website.

The user's name and password are convenient for authentication, but in more secure environments, they may have unacceptable limitations, such as the password being weak or easily guessed. In these situations, a more secure approach called "client-side authentication" may be used. In this approach, the user also possesses a private key and certificate and they are used, rather than a name and password, to authenticate the user's identity in the same way that the server authenticates its identity to the user's browser. This mutual authentication approach is more secure because it is far more difficult to guess the user's private key than it is to guess their password. The user's certificate and private key may be stored anywhere but are typically stored in a secure location which requires a password or some other secret to access it. In the case of the PIV/CAC cards, they are stored on the card and a PIN, entered by the user, is required to authorize the card to use the private key when it's needed to negotiate the secure connection. Used in this way, the user is said to be using a form of two-factor authentication, where the PIN is something the user knows and the PIV/CAC card is something the user possesses.

Client-side Authentication Setup

To enable client-side authentication, LiveWire must be given one or more digital certificates for the root certificate authorities that digitally sign the user certificates that LiveWire should trust. LiveWire will then accept any client certificate provided by a user that is signed by one of these root certificate authorities.

Optionally, the security of client-side authentication can be enhanced by enabling additional verification of client certificates using the Online Certificate Status Protocol (OCSP). When this protocol is enabled and a client certificate is presented to LiveWire, LiveWire will attempt to contact the certificate authority that signed the client's certificate to ensure it hasn't been revoked. To use this feature, OCSP information, in the form of a certificate extension, must be embedded into both the client's certificate and the root certificate authority's certificate. If either certificate lacks this extension, this feature cannot be used. Note that LiveWire has no control over whether or not the certificates contain an OCSP extension: The administrator must confirm its presence if they wish to use this feature.

The following steps are needed to enable client-side authentication. In this example, we use the NIST Test PIV Card PKI infrastructure, assume the administrator is using the Linux operating system, and assume the DNS name of the LiveWire appliance is `Omnipeek.` For a real PIV/CAC deployment, the DoD root certificates should be used, which can be found at *https://pkaps.pki.state.gov/webcardtest/downloads.aspx*.

> **Note** Your organization may use alternate or intermediate certificate authorities that require additional certificates.

To enable client-side authentication:

1. Obtain certificates for root certificate authorities.

   Obtain the certificate for each certificate authority that issues certificates to clients that you wish to allow access to LiveWire. Here, we download the NIST Test PIV Card root certificate which will allow LiveWire to trust users who are using those cards.

   ```
   curl -O https://csrc.nist.gov/CSRC/media/Projects/piv/documents/
   TestPIVCardsv2TrustAnchorRootCA.cer
   ```

2. Convert certificate(s) to PEM format.

   LiveWire requires that certificates be in the text-based PEM format. If one or more certificates is in an alternate form, such as binary DER, they must be converted. In this case, the certificate downloaded is DER format and must be converted with the following command:

   ```
   openssl x509 -inform der -in TestPIVCardsv2TrustAnchorRootCA.cer -out
   TestPIVCardsv2TrustAnchorRootCA.pem
   ```

3. Concatenate root certificates

   If more than one certificate authorities' certificates are to be trusted, their certificates must be concatenated into a single file (the "certificate bundle"). In our example, only a single certificate authority is trusted so concatenation is not required but we include it here for completeness.

   ```
   cat TestPIVCardsv2TrustAnchorRootCA.pem > client-ca.pem
   ```

4. Upload certificate bundle to LiveWire

   LiveWire assumes the certificate bundle is located at `/lib/ssl/liveaction/client-ca.pem` on the LiveWire appliance. Uploading is a multi-step process that requires administrator access to LiveWire.

5. Upload the certificate bundle to the appliance

   ```
   scp client-ca.pem admin@Omnipeek:~
   ```

6. Move the certificate bundle to the proper location

   ```
   ssh admin@Omnipeek sudo -S mv /home/admin/client-ca.pem /lib/ssl/liveaction/
   ```

7. LiveWire will detect the new certificate bundle and automatically restart with client-side authentication enabled. If you wish to disable client-side authentication, simply remove the certificate bundle:

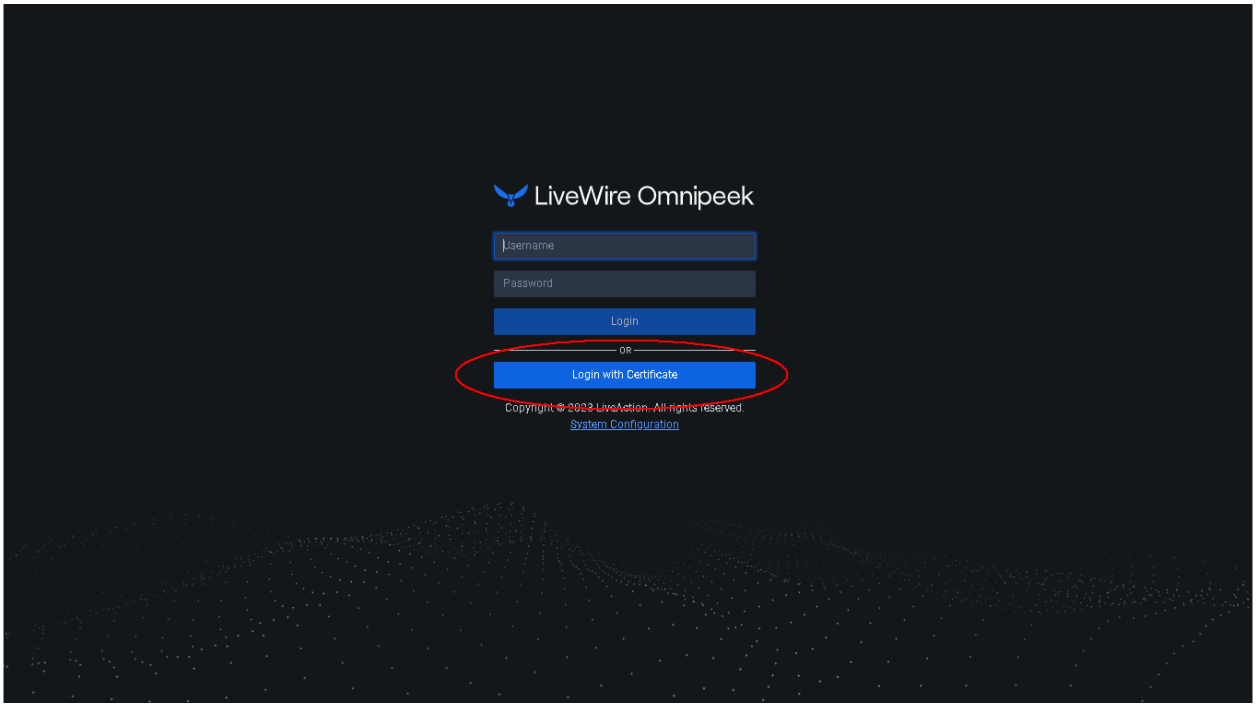
   ```
   ssh admin@Omnipeek sudo -S rm /lib/ssl/liveaction/client-ca.pem
   ```

Using the PIV/CAC Card

Once client-side authentication has been enabled in LiveWire as explained above, you can log into LiveWire Omnipeek using a PIV/CAC card associated with the account.

To use the PIV/CAC card:

1. From the LiveWire Omnipeek login screen, click **Login with Certificate**.



Copyright © 2023 LiveAction. All rights reserved.

2. Select your certificate if asked and follow the prompts provided by your PIV Card/CAC client middleware to authenticate to your card.

Enabling OCSP Support

LiveWire uses the NGINX web server to support OCSP. Enabling the feature requires modifying an NGINX configuration file.

To enable OCSP support, perform the following steps:

1. Connect to LiveWire and start an `ssh` session.

   ```
   ssh admin@Omnipeek
   ```

2. Modify the NGINX configuration.

   LiveWire uses the NGINX web server to support OCSP. Enabling the feature requires modifying an NGINX configuration file.

   ```
   sudo nano /etc/nginx/sites-available/omni-client-auth
   ```

3. Once the editor is loaded, add the following lines immediately under the `ssl_verify_client on`; directive near the end of the file and save the file. This enables the use of OCSP:

   ```
   ssl_ocsp leaf;
   resolver 8.8.8.8;
   ```

Note The IP address given by the `resolver` directive (in this example, a Google DNS server) must be the IP address of any DNS server capable of resolving the host names placed in each certificate's OCSP extension.

4. Restart the NGINX service. The new settings will not take effect until NGINX is restarted.

   ```
   sudo systemctl restart nginx
   ```

Local User Management

When a directory server is not available, local accounts may be used to allow users to log in. This method, however, is discouraged as it is has various limitations and is difficult to manage in environments with multiple appliances.

To allow login, a local account must be created for each user on each appliance they are allowed to access. The local account name must match the username portion of the UPN contained in the user's certificate. The UPN has the format `username@domain` much like an email address (in fact, in some scenarios, a user's UPN and email address are the same). The UPN can be retrieved from the certificate by loading the user's certificate is a certificate viewer. There are numerous viewers available on the Internet or use the Windows certificate viewer. Note that the domain portion of the UPN is ignored in this scenario so if two users have the same username but different domains, they will be indistinguishable from each other when logging in.

As an example, viewing the certificate from a specific NIST PIV test card, the UPN is given in the Subject Alternative Name extension as `32015465737401@upn.example.com.` Here, the username is the string of digits `32015465737401`. To allow this user to log in with a local account, create a local account on the LiveWire with the name `32015465737401`. It is important to note that, in this case, a local username comprised of only digits is considered invalid in a Linux environment so the creation of the local account must be forced. For this reason, the use of local accounts with PIV or CAC cards is discouraged.