SSL VPN

INTRODUCTORY USER GUIDE

Office of Communications and Information Technology

County of Sacramento
799 G Street
Sacramento, CA 95814

1 INTRODUCTION

This guide is provided to introduce you to the County of Sacramento's Secure Socket Layer (SSL) Virtual Private Networking (VPN) solution, otherwise known as SSL VPN.

SSL VPN is a "clientless" solution in that it does not require a formal client installation as past County VPN solutions have required. It does, however, require the activation/installation of certain ActiveX/Java elements which will be covered in this document. This is done in an automated fashion requiring little user interaction making the solution extremely easy to use.

SSL VPN is also browser based. This means any current web browser can be to access SSL VPN. DHHS supports Internet Explorer 6 and 7.

2 SSL VPN USE

SSL VPN provides County of Sacramento staff remote access to County Resources. Its use is governed by both County and applicable departmental policies. Users of the service must use in accordance with these policies[1] and for the purposes it was granted.

When utilizing County managed or known personal assets, SSL VPN provides a streamlined means of access County Data and Systems. This provides the County's workforce an unprecedented means of working mobility.

With this mobility, additional caution should be exercised in where SSL VPN is used from. SSL VPN provides the ability to be far more mobile than the County's prior client-based solution. Any resource with a supported web browser can access SSL VPN. While there certainly are several security controls for SSL VPN, users should avoid its use in areas of high risk or on questionable systems. Environments that fall into this category may be any of the following

- Public Kiosks
- Public Access PCs
- Other questionable or unfamiliar computing environments

3 OVERVIEW

The following is an overview of the SSL VPN portal and its key functions. More detail, if required can be provided by departmental MIS Staff.

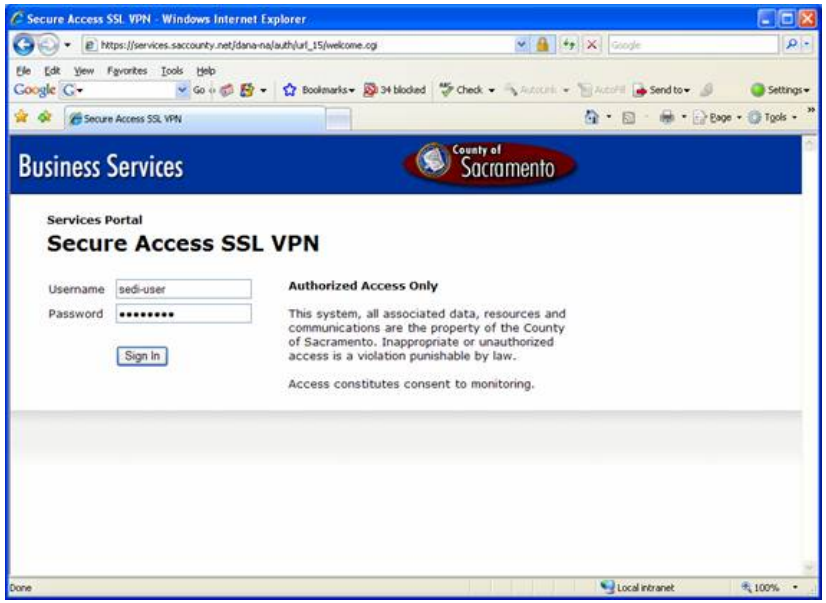
[1] County IT Security Policy and SEDI – SSL VPN Remote Service End User Agreement.

The access portal for SSL VPN can be reached by entering the following URL into your web browser (Internet Explorer 6 or 7 only).

http://services.saccounty.net

Authentication is performed by entering the username and password.

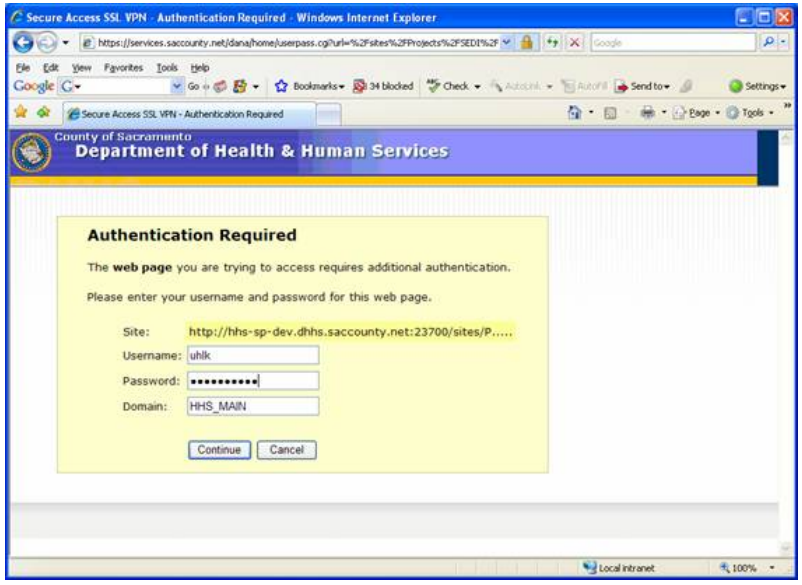
After entering this information simply click sign in to begin your SSL VPN session.



The next screen displayed requests authentication to the DHHS AD domain which is required to access the SEDI Portal.

Authentication is performed by entering the username and password.

After entering this information simply click Continue to connect to the SEDI Portal.

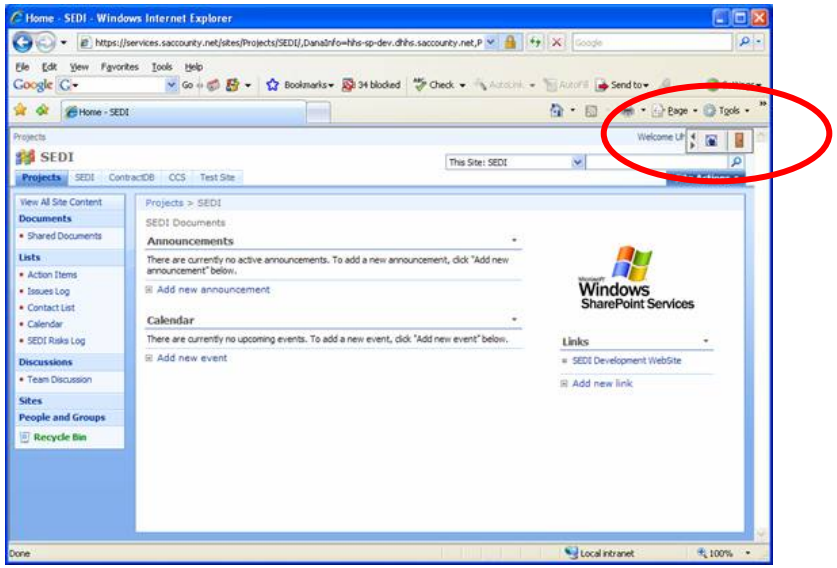


SSL VPN Tool Bar

The primary SSL VPN Toolbar provides some easy to use tools.

Home: Navigates to the main portal view

Sign Out: Used to properly terminate your SSL VPN session.



4 CONCLUSION

The purpose of this document was to provide a friendly introduction to the SSL VPN portal. As users become more familiar with the interface its ease of use will also increase. If you have questions or concerns not addressed in this introduction please contact the DHHS Support Center at 916-875-6123.