IET - Communications Resources
Service Level Agreement for SSL VPN

The purpose of this Service Level Agreement (SLA) is to establish a cooperative partnership between IET - Communications Resources and the client department by clarifying roles, setting charges and expectations, and providing mechanisms for resolving service problems within a specified and agreed upon time period.

1.0 Overview

This SLA is between IET - Communications Resources (CR) and a client department. Under this SLA, CR agrees to provide, at the specified price and duration, SSL *(Secure Socket Layer)* VPN *(Virtual Private Network)* service to allow departmental VPN Administrators to configure SSL VPN for their campus department on the backbone network. SSL VPN services will allow remote access to authenticated users to their department Web-based applications or to campus Web-based applications. SSL VPN offers clientless access to Web-based applications via a Web browser.

This SLA also covers performance, reliability, and other topics pertinent to the SSL VPN; in particular, it lists key responsibilities of CR and its client departments.

2.0 Funding of Services

A minimum of 15 user licenses is required for SSL VPN service. One-time and monthly charges assessed for SSL VPN appear below.

Initial Charges

SSL VPN Installation	$274.50
License Initiation Charge *(Minimum of 15)*	$6.50 per license

Monthly Recurring Charges

License Charge *(Minimum of 15)*	$11.50 per license

Reconfiguration Charges

Change/Modify # of Licenses	$40.00

The service charges assessed for SSL VPN service will appear on the Monthly Telecommunications Billing statement. Installation is complete within five (5) business days of Service Order creation. The customer will incur service charges as soon as installation is complete. Charges will be reviewed annually at the start of the fiscal year, July 1.

3.0 Terms of Agreement

This SLA is for one (1) fiscal year, beginning on July 1st and extending to June 30th of the following calendar year. Both parties (CR and the client department) must review and agree on terms in order to extend the SLA on an annual per-fiscal-year basis. CR will notify the client department three (3) months prior to any alterations to the agreement.

In the case that the needs of a client department are not covered in this SLA, a custom SLA can be negotiated. The SLA must be accepted and signed by both parties 90 days prior to its execution.

4.0 Communications Resources Responsibilities

IET - Communications Resources shall:

4.1 Allow users to connect to their campus department LAN via SSL VPN connection.

4.2 Configure *only* basic settings to establish SSL VPN service such as domain and VPN Administrator account, license limits and IP address. The departmental VPN Administrator will be responsible for more detailed SSL VPN configuration for their campus department.

4.3 Install, and maintain the backbone equipment and backbone as covered by this agreement, or as deemed appropriate by CR, if not covered. Additionally, provide programming and network administration support necessary to install and maintain the backbone infrastructure hardware and software, as covered by this agreement.

4.4 Facilitate customer requested user license changes to the SSL VPN for the aforementioned reconfiguration charge (see Section 2.0).

4.5 Provide 24 x 365 monitoring and maintenance of the hardware and supported protocols.

4.6 Diagnose all reported SSL VPN problems when related to backbone equipment.

5.0 Client Department Responsibilities

Client Departments shall:

5.1 Submit a completed Service Order to IET - Communications Resources with an authorized signature, and provide the name and contact information of the person who will be the departmental VPN Administrator. The departmental VPN Administrator will be the CR contact in the client department for the installation.

5.2 Provide to CR the email, pager, and phone contact information for the departmental VPN Administrator and a backup administrator. Any changes to these contact/notification methods must be communicated to IET - Communications Resources.

5.3 Provide first-level network support to users in the client department.

5.4 Diagnose all reported SSL VPN problems when related to backbone equipment.

5.5 Be responsible for the detailed configuration of the SSL VPN settings for their campus department.

5.6 Track user data and administer services, resolve conflicts between users, and correlate IP addresses to individual machines.

5.7 In consultation with others, and as necessary, handle violations of campus computer use and security policies by service users.

5.8 Submit Service Order for any change required in the SSL VPN configuration.

5.9 Be responsible for any charges from CR for diagnosing problems that fall under the responsibility of the client department.

6.0 Maintenance, Performance and Problem Resolution

- Except as covered below, CR will ensure availability of the SSL VPN service on a 24 x 365 basis.
- In general, availability will only be changed by negotiation between the client department and CR. In the rare circumstance that CR must alter system availability, the departmental Network Area Resource (NAR) will be notified as soon as possible.
- The departmental NAR will be notified via email if any network maintenance is required. Planned network maintenance may result in complete lack of connectivity for all customers.

- If a client department experiences a problem with their SSL VPN connection and needs assistance, the departmental VPN Administrator or Network Area Resource (NAR) should contact the IT Express Computing Services Help Desk at 530-754-HELP (4357).
- Normal business hours are 8 a.m. to 5 p.m., Monday through Friday. Campus after-business hours are 5 p.m. to 8 a.m., Monday through Friday, and from 5 p.m. Friday through 8 a.m. Monday. Designated campus holidays will be staffed as after-business hours. Support is provided after-business hours by on-call technical personnel. CR will take appropriate action to restore performance according to CR Service Prioritization.
- In the event that there is a campus network problem affecting the client department's connection, the departmental NAR will be notified via email to the technotices@ucdavis.edu listserv. The departmental NAR will not be contacted directly.
- Unscheduled downtime for any segment of the SSL VPN service due to unscheduled outages is targeted to not exceed one percent (1%) of scheduled availability during the SLA period (one year). Service interruptions caused by conditions outside the control of CR (e.g., vandalism or fire) will be handled to the best ability of CR.
- When performance measures do not meet the standards specified in this SLA, the client department and CR will jointly work to:
    - Identify the cause of the problem.
    - Resolve the problem as quickly as possible

7.0 Upgrades

Software and hardware upgrades are at the discretion of CR and cover the network backbone hardware and SSL VPN hardware. These upgrades will be made with minimal disruption of service.

8.0 Accountability

CR warrants that all reasonable measures within its resources shall be taken to ensure the performance, availability, and integrity of the SSL VPN service as covered in this agreement. CR assumes responsibility for the hardware and software that it provides to execute this SLA, as well as for the actions of CR staff. CR's liability for damages is limited to hardware replacement or repair, software fixes, and corrections to staff errors.

The departmental VPN Administrator and client department agree not to configure the SSL VPN domain space in a manner that compromises the campus backbone or violates security or other applicable policies. The client department also assumes responsibility for any misuse of their LAN by users and will remedy any such situations.