Information Technology Council
Humboldt State University

Meeting Notes for: April 14, 2009 from 2:00 to 4:00 P.M., NHE 116

Members Present: Mark Hendricks (Chair), Dave Pearson (CPS), Chris Hansen (CAHSS - proxy for Megan McKenzie), Greg Osburn (OEM - Dale Sanford, Toby Walker (SA), Colby Smart (HR), Jeremy Shellhase (Library), Jeanne Wielgus (DITSS), Scott Ventuleth (TNS – proxy for Rick Garcia), Dave Marshall (CNRS), Drew Myer (Housing), John Filce (OAA)

Others Present: Ed Gordon (UPD), Josh Callahan (CITSS), Shawn Kohrman (DITSS), Molly Simpson (Recorder)

1. Approval of the Minutes:

March 10, 2009 minutes were approved as distributed (Shellhase/Wielgus).

2. Report Items:

DSWAG: Adorador updated the Council on antivirus testing noting that test servers are up and running. Products being tested are Symantec, Sophos, C.A., and MacAfee. Documentation will be forwarded to DSWAG members on Wednesday.

Hendricks reported that the Kbox ticketing system is currently being used by ITS and is working well. He also noted that the DSWAG is working on Active Directory best practices. The group is currently reviewing information provided by Hendricks.

NAG: Meyer reported that the group had been testing the new Internet facing change form which is now available on-line.

Hendricks noted that the closed border internet facing server page is available. To date, no requests for exceptions have been received. He reminded Council members that the form must also be reviewed for existing exceptions. The form has been available since April 1st, 2009. More information is available on the Security page.

The group meets again next Thursday at 2:00 P.M. JGC, 2nd Floor, Mad River Room.

Encryption Working Group: Hansen reported that the group had their first meeting on April 8th. The group came up with a matrix that identified where encryption might be used. The group also discussed encryption related issues that the campus faces:

- There is currently no campus policy relating to the encryption of data on campus systems and devices.
- Additional training related to protected data and responsibilities.
- Private Key Infrastructure (PKI) is essential for most encryption applications. Callahan and Hendricks discussed developing a PKI infrastructure for HSU. Callahan obtained quotes that indicate a cost of greater than $50K for the campus. They are attempting to obtain CSU buy-in on a CSU wide PKI.

The group reviewed OS and volume supported encryption options. New versions of Vista and Windows 7 will support encryption with Active Directory (AD). This applications known as "Bit Locker" can make use of hardware modules known as TPM that allows the entire dist to be encrypted at the BIOS level. Bit Locker used with AD will also support encryption key recovery at the domain level. It is recommended that any computer purchased by the campus contain TPM support. The Mac solution, known as "File Vault" used the user's password to generate the encryption key. Because this key may be lost when the password is changed, and because File Vault currently does not have the ability to perform encryption key recovery, it does not appear to be a recommended option for the campus. Level 1 and Level 2 data should not be saved on Mac OS X systems until File Vault will support key recovery or unless some other encryption application is used.

3. Discussion Items/ Action Items:

ITRP2 Update: Ventuleth updated the Council on ITRP2, noting that the project is falling behind schedule; TNS is trying to get all the deliverables back to AT&T before the final project plan can be published with timelines and approximate dates.

Ventuleth noted that TNS recently received firewalls that will eventually protect the datacenter VLANs.

TNS is in the process of shutting down inactive ports in preparation for ITRP2 access layer. Ports will be shut down if the following criterion is met:

- Chancellor's office shows no port activity
- The jack is not in a conference room or classroom
- No billing service record exists

He also noted that the wireless component is slowly moving forward with jack installations in campus buildings. Buildings that are ready to have access points deployed once refresh is done now include: Wildlife, Harry Griffith, Founders, Library, Social Sciences, Kinesiology, and Science A.

Host DHCP configuration is part of CSU standards and will go live at refresh time. Hendricks asked what the current approval process is for these standards.

Change Management Procedure: Callahan presented the change management procedure reviewing the life cycle process for enterprise systems. The procedure has been revised and expanded. This document has been presented to the Council for the 30-day review process. Please send comments to Callahan.

4. New Business:

SMTPS Instruction and Schedule: Kohrman referred to the attached document for SMTPS instructions and schedule. The effective date will be October 18, 2009 for off campus and April 18, 2010 for on campus.

MS Information Rights Management Services: Pearson brought forward a request from his constituents to evaluate the feasibility of MS Information Rights Management Services. This software allows controls on editing or forwarding. It also tracks who viewed or printed documents by locking document at the file level. Requirements are licenses for all who send/receive as well as a .net account. Discussion ensued. Consensus was that this product was not feasible to implement or support.

Web Migration Update: Callahan reported that the timeline and documentation for web migration where in place.

- The *Sorrell* replacement will be *Central Server*. This server will be split into two separate clusters. One for Official University Communications and the other one for Users – Network Folders.
- Drupal 6 will be available for content management by campus users after they have completed the required ATI training.
- "~ "addresses in the current system will be supported in the new environment; however, new accounts will not use the "~".
- Accounts will be automatically generated through Account Center (formerly WebReg)
- ATI training will be required for new accounts and for developers.

Hendricks stated that this is a major change especially for campus areas doing programming. The Web office will move over at the beginning of this summer.

5. Announcements:

IT Council Membership Changes: Hendricks informed the Council of recent changes to the membership:

- Colby Smart - representing Human Resources
- Scott Gerving – representing University Center
- Mark Hendricks – now appointed to the ISO seat formerly held by McBrearty

Monthly Maintenance Window: Hendricks reported that the next maintenance window would be Sunday, April 18th from 5:00 A.M. to 11:00 A.M. He told the Council that every major system with experience some down time.

Colo Logs: Walker asked if ITS currently maintains logs for patches and updates on collocation servers. If not, it would be beneficial to begin this practice for auditing purposes. Callahan noted that current collocation service level agreements were being standardized and will include terms and services provided.

CSU-CO Information Security Awareness Training: Hendricks asked for feedback on the new on-line training for IT Staff. Marshall noted that requiring the participant to comply with policy would be more effective if the training module pointing to this policy.

Closed Border Project Status Report: Already covered under NAG report.

6. Adjournment: 2:58 P.M. (Pearson/Smart)

Encryption Working Group

4/8/2009

Present were Callahan, Hendricks, Osburn, and Hansen.

Our first meeting was mainly a general discussion of terms and the likely areas where we should consider encryption issues. These areas ranged from file- and folder-level encryption; email, code- and digital signing; wireless, SQL, and SSL network communications, VPN and other network tunneling; database encryption, either at rest, or data-level encryption; and filesystem encryption within separate volumes, separate file storage, portable devices (laptops, smartphones) and removable storage (optical, USB, and other drives.)

A component central to several of these areas is to have a **Public Key Infrastructure** (**PKI**), a set of hardware, software, people, policies, and procedures needed to create, manage, store, distribute, and revoke digital certificates. We conjectured that the CSU as a whole might do that, or it might fall to HSU.

The Chancellor's Office IS Office has reported recently that they have an encryption working group. No firm details yet. We plan to gather some more information on that working group.

We are also going to find out what other CSU campuses are doing, as it is an awfully big wheel to try to reinvent.

User security awareness and training will be an important component to encryption, and we consider the practices of the user to be at the top level of our discussion framework.

What are some encryption product possibilities? Early candidates for consideration (the no-cost options ;-)

BitLocker (Windows Vista, included with Vista Enterprise, requires either Server 2008, or AD schema additions to Server 2003 with the changes expected to align with preparation for an eventual move to 2008 server.)

FileVault (Macintosh, included with OS X 10.3 and higher)

TrueCrypt (Open source, supports Win/Mac/Linux)

Among our concerns regarding solutions:

Functionality that maintains usability, encryption that does not defeat the user experience,

Supportability, recovery of encrypted data by trusted others

Standardization, reducing overall support and increasing integration across campus and CSU.

Longevity, that is not locking in to a 3rd party vendor that dries up, or proves incompatible in some larger context.

It was noted that the CSU and HSU do not have a clear policy on encryption yet, and thought that there should eventually be policies regarding the storage and transmission of confidential or restricted data.

Several Windows whole disk encryption products either support or require the presence of a **Trusted Platform Module** (TPM). Full disk encryption applications, such as the PGP Whole Disk Encryption and BitLocker, can use this technology to protect the keys used to encrypt the computer's operating system volume and provide integrity authentication for a trusted boot pathway (i.e. BIOS, boot sector, etc.) We might explore adding the TPM to future hardware standards for campus computers.

We will be meeting in another month.

This group is open to interested parties. The initiation is to bring snacks.

IT Council Agenda

Next Meeting: Tuesday, April 14th, 2009
Location: *NHE 106*
Time: *2:00 P.M.*

I. Approval of the Minutes

http://www.humboldt.edu/~its/planning/committees

II. Working Group Report Items

1. Desktop Support Wk Group (DSWAG): Hendricks
2. Network Advisory Group (NAG): Meyer
3. Encryption Wk Group: Hansen

III. Discussion Items/Action Items

1. ITRP2: Garcia
2. Change Management Procedure: Callahan

IV. New Business

1. SMTPS Instructions & Schedule: Rizzardi
2. Microsoft Info Rights Management Services: Pearson
3. Web Migration Update: Rizzardi

V. Announcements

1. IT Council Membership Changes
2. Monthly Maintenance Window: Hendricks
3. CSU-CO Information Security Training: Hendricks
4. Closed Border Project Status: Hendricks

VI. Adjournment

HUMBOLDT STATE UNIVERSITY

HSU-IT-Procedure:
Enterprise Services Change Control
Status: DRAFT Procedure
Proposed Classification: Required

1.0 Purpose
The purpose of this procedure is to define the process for approving changes to Enterprise Services.

2.0 Scope
This procedure establishes the approval and review process for both System and Application level changes to Humboldt State University's Enterprise Services.

2.1 Intended audience
Changes made through this process will be initiated by ITS, and other campus ITCs, but could affect all users of Humboldt State University's Enterprise Services.

3. Procedure
3.1 Enterprise Service Lifecycle
3.1.1 Initiation: New Services shall be established and resourced by the ITS Management Group before entering the Planning phase
3.1.2 Planning: This phase encompasses development, implementation, and pilot testing of the Service
3.1.3 Delivery: When the Service is ready for production, the implementation team shall provide the Help Desk with documentation, primary and secondary support contacts, and any other relevant operational information at a Delivery Briefing.
3.1.4 Operation: All changes to an Enterprise Service that has been Delivered shall go through this Change Control Procedure.
3.1.5 Renewal: Once established, each Enterprise Service needs to be renewed and prioritized on the Mission Critical Server list annually.
3.1.6 Decommissioning: If a Service is not renewed, ITS shall communicate a decommissioning timeline lasting at least one month to the Service's users.

3.2 Change Requests
3.2.1 Change Requests shall be initiated using the Humboldt State University: Enterprise Service Change Request Form (included as Attachment A).
3.2.2 Emergency Changes triggered by Security Incidents will be handled as Emergency Changes and will be reviewed by the Enterprise Services Advisory Group post-implementation
3.2.3 Non-Emergency Changes will be reviewed by the Enterprise Services Advisory Group before implementation.

3.3 Change Windows
3.3.1 System Changes: There shall be one (1) window for System Changes scheduled for the third Sunday of each month from 5:00 A.M to 11:00 AM.
3.3.2 Application Changes: There shall be two (2) windows for Application Changes each week, Tuesday and Thursday evenings from 5:30 PM to 7:00 PM
3.3.3 Business Hour Changes: In cases where external support (e.g. Vendor Technical Support) or key resources are not available outside of normal HSU working

hours, changes can be scheduled during Business Hours provided that at least 48 hours notice is given to the Service Users and that the campus academic calendar and relevant business functions are scheduled around as much as possible.

3.4 Change Control Group

3.4.1 The Enterprise Services Advisory Group, a standing technical working group will be delegated the responsibility to review and discuss System and Application Change Requests for Enterprise Services. This group's decisions will be presented monthly as an IT Council Agenda item for recommended implementation by ITS Operational Staff during the next appropriate change window.
3.4.2 Membership: The group membership will consist of members or designees from the following areas: Central IT Systems and Services, Desktop IT Systems and Services, and the IT Council

3.5 Change Management Process

The Change Management process is comprised of six steps:

3.5.1 Planning: This step lays out the specific tasks, sequences, and responsibilities that must be completed for a successful change. Prerequisites and dependencies are identified and specific times are also indicated where tight coordination is necessary
3.5.2 Approval: This process is intended to verify that all of the steps defined in the request process have been carried out and are appropriate in view of the risk and impact to the organization.
3.5.3 Schedule: In this process, all approved changes are scheduled on a master activity schedule to enable all affected resources to be aware of the activities planned for the Enterprise Services environment. It also allows conflicts of resources and major impacts to be reviewed and revised, when necessary.
3.5.4 Implementation: This part of the process establishes a mechanism in which changes can be applied in an effective, high-quality manner, and basic pre-scripted tests of functionality can be informed.
3.5.5 Backout: This part of the process specifies a mechanism whereby changes can be entirely removed if necessary without adversely impacting the system's ability to perform in the same manner as before the change. As needed, it will imply preparatory steps such as the creation of a complete backup image or storage of configuration files in a secure location, prior to the change being applied.
3.5.6 Review: This part of the process assesses the successful implementation of the change. Was the change completed on time and correctly? What if any problems were encountered? What processes and/or procedures may require modification to ensure successful completion in the future?

3.6 Approval Criteria

3.6.1 State of the Production Environment: Before determining if a change should be approved, the change control group evaluates the performance and availability of each Enterprise Service since the last window.
3.6.2 Change Level: As part of the approval process, the change level is examined along with the detail information and instructions attached to the change request. The attachments should detail the associated risk and impact of the change.
3.6.3 Aggregate Effect of Proposed Changes: The change control group is a forum where all of the changes requested for each change window come together. When there is an unacceptable composite risk from multiple proposed changes, the group's responsibility is to prioritize the changes and reschedule some.
3.6.4 Resource Availability: The group should be concerned about the availability of time, people and resources when considering the scheduling and approval of changes.
3.6.5 Criticality: There are issues that may alter the impact of the change. For example the change author may feel that the impact is relatively low because his change affects a small percentage of the user community. Conversely, a security patch could be rated as highly critical due to the risk creating by not applying it.

3.7 Change Levels

There are three major levels which are used to define changes:
Level 1, System Changes: These are the most significant changes, all hardware changes, operating system upgrades and patches and application upgrades are in this category. These changes are limited to the monthly change windows, contingent upon approval by the change approval group.
Level 2, Application Changes: These are changes to how an application is configured, how a service operates, and minor application level patches. These changes can be scheduled during the bi-weekly Application Change windows if they are approved by the change approval group and communicated to the affected user base in a timely manner.
Level 3, Operational Changes: These are common changes that occur frequently and are normally non-disruptive or administrative in nature. Backout is readily available and reliable. Level 3 changes do not require Change Control paperwork or Change Control Group approval but should be documented in a Change Log designated for that Service.

It is the responsibility of the technician or author of a change request to evaluate it against the following six categories and assign the Change Level. While the change author normally has a technical perspective with respect to these categories, a business perspective must also be applied when assigning a level. The six categories are:

Risk, which considers the possibility of success based on the difficulty and complexity of the implementation and back out procedures.
Impact analyzes the overall impact to the organization based on the machine and people resources.
Communication Requirements takes into account which part(s) of the campus community need to be notified of the change and what the logistics are for adequately notifying the affected parties.
Install time considers the overall time requires to prepare and implement the change as well as to recover from a failed change.
Documentation assesses the degree to which procedures must be amended to adequately describe what has changed.
Education/training needs considers how significant an impact the change will have on those using or operating the system and what it will take to reasonably expect them to adapt to the new situation.

4.0 Compliance

The CMS Project Director and the Directors of Central IT Systems and Service and Desktop IT Systems and Services are responsible for compliance in their respective areas.

5.0 Enforcement

The CMS Project Director and the Directors of Central IT Systems and Service and Desktop IT Systems and Services are responsible for enforcement in their respective areas.

6. Definitions:

Term	Definition
Enterprise Services	Systems that provide core services used across the institution and on which other applications often are dependent.
Humboldt State University Enterprise Services (e.g.)	CRM, Data Warehouse, Cashnet, Banner, Document Imaging, Central Web, E-mail, Learning Management, DHCP, DNS, and

	Directory Services
Application Change	A change which can be made to the configuration of a software package which requires that application, subsystem, or service to be restarted, but does not require the underlying operating system to be restarted.
System Change	A hardware or operating system change which requires a restart of the system or which could affect the behavior or functionality of all software packages hosted on that system.
Change Window	A defined period during which changes that could potentially disrupt service are conducted.

Document History

Action	**By**	**Date**
Adapted to ITC Procedure Format	**Josh Callahan**	03/03/2008
Updated	**Josh Callahan**	03/28/2009,04/07/2009
Draft Procedure		
RFC Draft Procedure Posted for IT Council	**ITC: Working Group**	**Date**
Recommended Procedure Approved by IT Council	**IT Council**	**Date**
Procedure Approval	**CIO/ISO**	**Date**
Posted		**Date**
Reviewed		**Date**
Obsoleted		**Date**

Attachment A: Humboldt State University: Enterprise Service Change Request Form

HUMBOLDT STATE UNIVERSITY

Enterprise Service	
Software/Hardware Subsystem	
Description of Change	
Change Level	Level 1: System Change _____ Level 2: Application Change _____
Change Window Requested	
Emergency Change	Yes No

Change Author's Signature, Title	**Date**
Spo	**Date**

The following section is to be completed by the Enterprise Services Advisory Group:

Change Request Security Review Results
Change Request Results: Approved/Denied, and Comments

March 26, 2009 DSWAG Meeting Summary

1. ITS Ticketing Referral Procedure

   Shawn Kohrman presented a procedure draft for the way the help desk will make referrals to ITC support outside of ITS. It was asked that steps be included for making it explicit to the user/requester that a referral does not imply a specific action being taken. For example when someone requests a software install in a specific time frame (the 12:33 "My friend brought me a Creative Suite 4 DVD and I need installed before my 2 o'clock class" syndrome); the fact that a referral was made should not leave the impression that the software is approved for installation nor that it can be installed as soon as requested.

   Shawn said he will create, and present in the next DSWAG meeting, a boiler plate for ITS communications to users who initiated referenced requests.

2. Antivirus Solution Evaluation

   John Adorador contacted Computer Associates, McAfee, Sophos and Symantec for proposals with the following considerations:

   - Manageability with reporting and updates for platforms: Win 2000+, OSX 10+, Linux, Win Server 2003 and 2008 – including 64bit
   - Once a day update intervals for all platforms.
   - Licensing by host or by OS
   - Compatibility with Bradford, Oracle, SQL, MySql,
   - AD and ARD deployable
   - Responsive customer service
   - Low CPU usage and small resource footprint
   - Integration with KACE KBOX
   - Different levels of management console (departments, colleges, etc.)
   - Support structure that allows multiple (>=5) campus contacts

   John requested each vendor provide pricing at these levels of coverage:

   i. Campus owned equipment
   ii. Campus owned + Faculty/Staff owned
   iii. Campus owned + Faculty/Staff owned + Student Owned

   Not all vendors had supplied the requested quotes before the DSWAG meeting; but each appears to warrant testing based on meeting the minimum requirements (based upon vendor claims). John and others in ITS will setup servers so **testing** can be **completed in April**. We are on schedule for evaluations to be discussed at the next DSWAG meeting resulting in **a recommendation with justifications being provided to Anna Kircher prior to the IT Council meeting in May.**

3. Active Directory Best Practices
   Mark Hendricks presented an outline for OU and GPO best practices that was based on conversations from last year. It was agreed that forced logouts, firewall exceptions and other GPO controls be discussed in the next DSWAG meeting. The intent is to communicate what the different organizations are doing and discuss ideas – not create mandates.

March 19, 2009 – Meeting Summary

Attendance: Mark, Tom, Miles, Shawn, Rick, Chris, Drew, Dave R, Jeanne

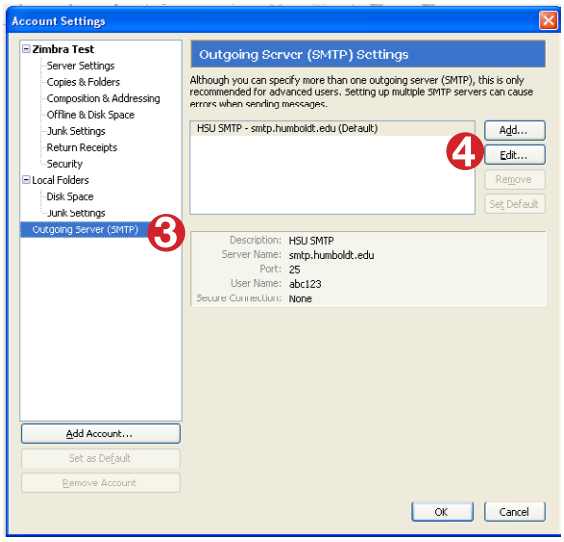
1. TNS showed a preview of the On-Line form for Internet Facing Server & Firewall Change Form
    a. We were able to test and found some issues.
    b. It's now online and ready.
        i. https://tns.humboldt.edu/ifd/itc_logon.php
    c. Mark H. thought this might be an effective tool for setting up rules on the new Data Center firewall that is being installed as part of ITRP2.
        i. More information was needed to find out if this is a possibility.

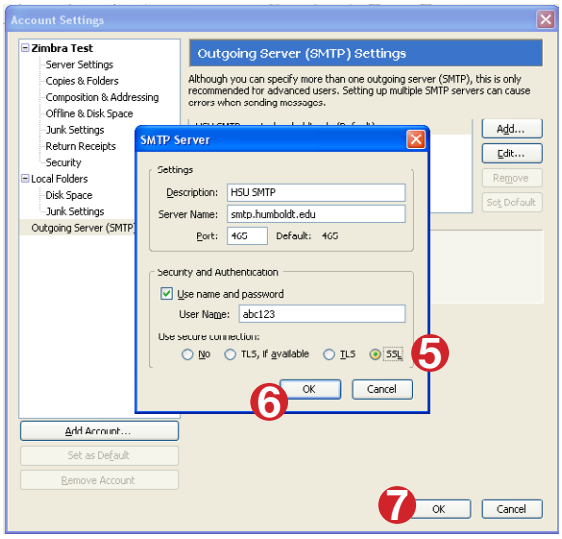
2. TNS wanted to inform IT community of changes to the Old Campus Network (Pre TII)
    a. Old IP address used on the old network will be reclaimed and needed for ITRP2
    b. Campus Houses are affected and left on the old campus network
    c. Switch over to a new VLAN and issue new IP address's
    d. TNS will coordinate with ITC's that have hosts in those areas.

3. ITRP II Updates
    a. Reviewed the Timeline of project that was sent out by Rick G.
        i. Original was confusing. Rick G. Looking into getting a more concise version.
    b. Rick G. provided a Wireless implementation update.
        i. Priorities have changed because of funding.
        ii. Library is ready
        iii. AP's will be deployed in areas that have easy access. Areas that don't need core drills, new penetration through walls, etc.
        iv. Rick G. will provide a listing of those areas.

Secure Outgoing Mail (SMTP) Setup Guide

Mozilla Thunderbird – Windows*

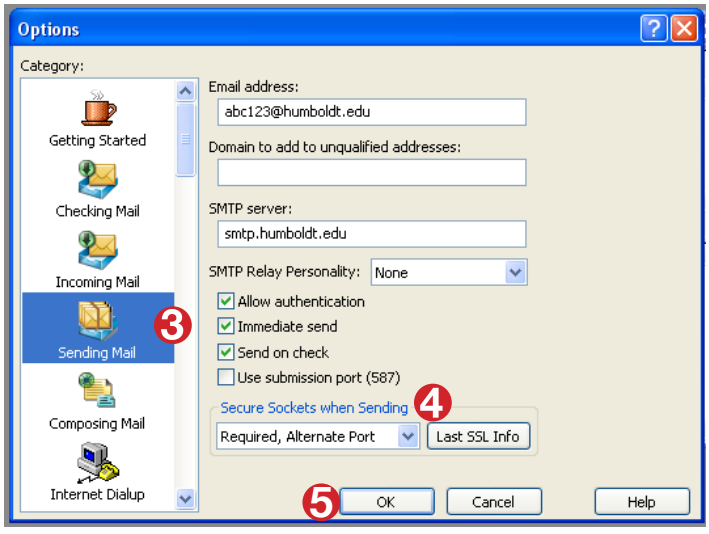




1. Load Mozilla Thunderbird.
2. In the **Tools** pull-down menu select **Account Settings…**
3. In the left hand panel select **Outgoing Server (SMTP)**
4. Click the **Edit...** button.
5. Select the **SSL radio button** in the **Security and Authentication** section.
6. Click the **OK** button for the **SMTP Server** window.
7. Click the **OK** button for the **Account Settings** window.

**This software has been removed from our Supported Clients list because of the limited functionality (no calendar support, no synced address books, no shared address books). After this project, we will not be providing instructions for this software.*

Eudora – Windows*



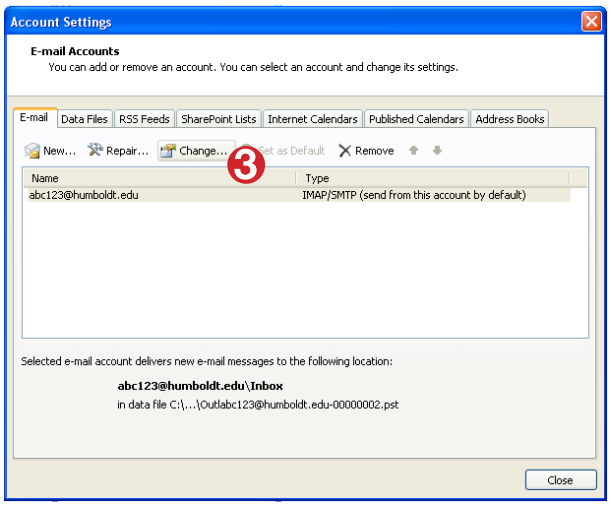
1. Load Eudora for Windows.
2. In the **Tools** pull-down menu select **Options…**
3. Select the **Sending Mail** category.
4. On the **Secure Sockets when Sending** pull-down menu select **Required, Alternate Port**.
5. Click the **OK** button.

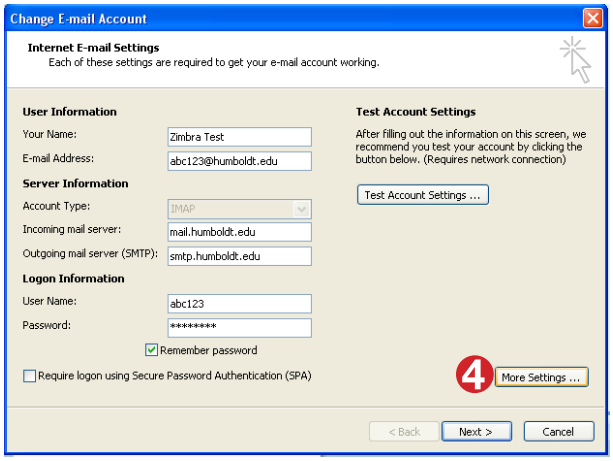
**This software has been removed from our Supported Clients list because of the limited functionality (no calendar support, no synced address books, no shared address books). After this project, we will not be providing instructions for this software.*

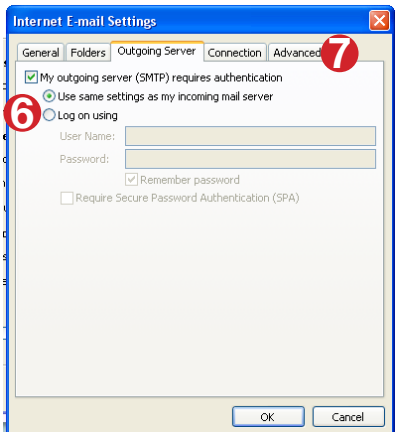
Microsoft Outlook 2007

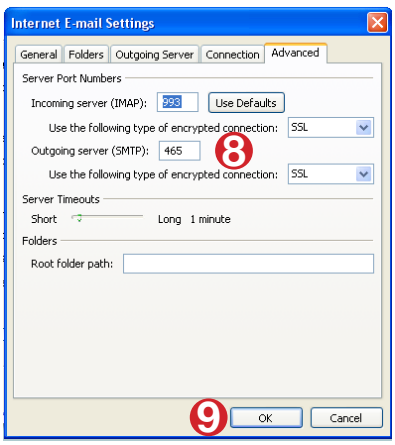
Please note: These steps are not required if you are using the Zimbra plug-in for Outlook.

1. Launch Outlook 2007.
2. In the **Tools** pull-down menu select **Account Settings…**
3. Select the **Email** tab and click the **Change…** button for the account.
4. In the **Change E-Mail Account** window, click the **More Settings…** button.
5. Click the **Outgoing Server** tab within the **Internet E-Mail Settings** window.
6. Check the box for **My outgoing server (SMTP) requires authentication.** Make sure the **Use same settings as my incoming mail server** radio button is checked.
7. Click the **Advanced** tab within the **Internet E-Mail Settings** window.
8. Set the **Outgoing server (SMTP) port** to **465**. Set the **Use the following type of encrypted connection** to **SSL.**
9. Click the **OK** button for the **Internet E-Mail Settings** window.
10. Click the **Next** button in the **Change E-Mail Account** window.
11. Click the **Finish** button in the **Change E-Mail Account** window.
12. Close the **Account Settings** window. You should now be back to Outlook 2007.









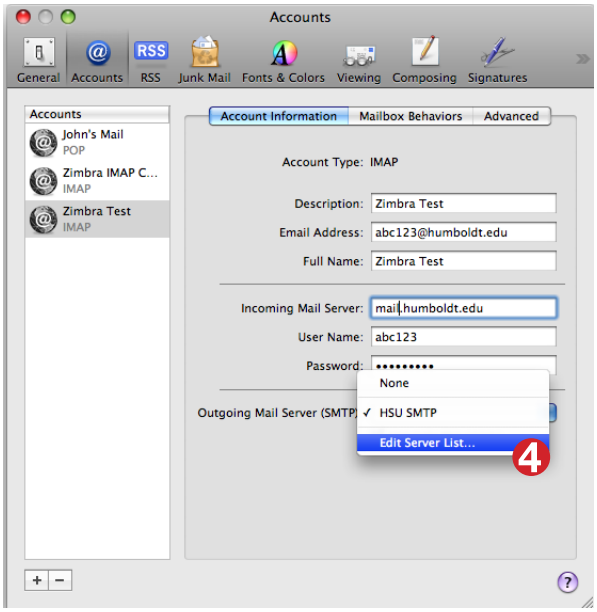
Macintosh Mail (Mac OS X 10.5)

1. Launch Apple Mail.

2. In the **Mail** pull-down menu, select **Preferences.**

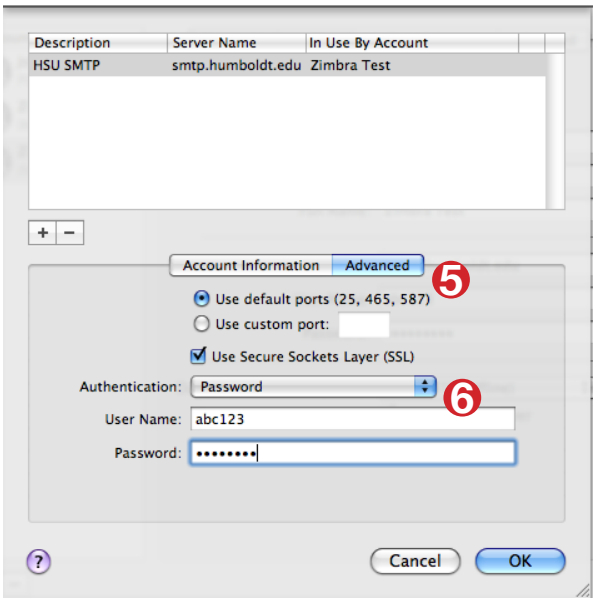
3. Click the **Accounts** category.

4. Select the pull-down menu for **Outgoing Mail Server** and select **Edit Server List.**

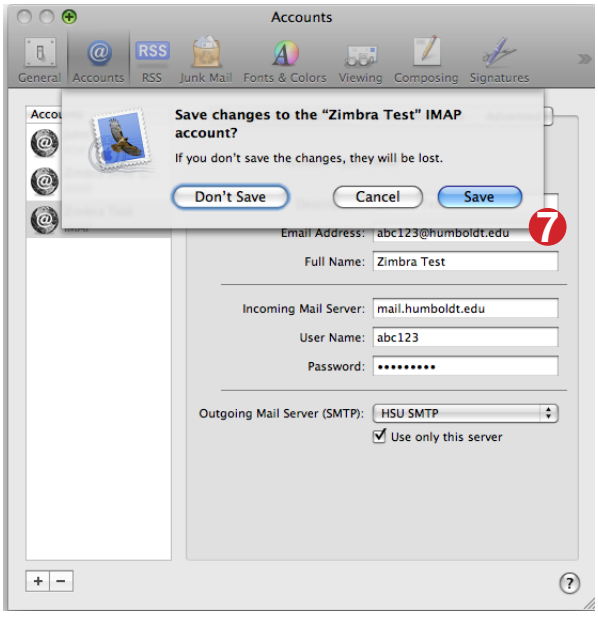


5. Click the **Advanced** tab. Make sure the **Use default ports (25, 465, 587)** radio button is selected. **Click the Use Secure Socket Layers (SSL)** box.

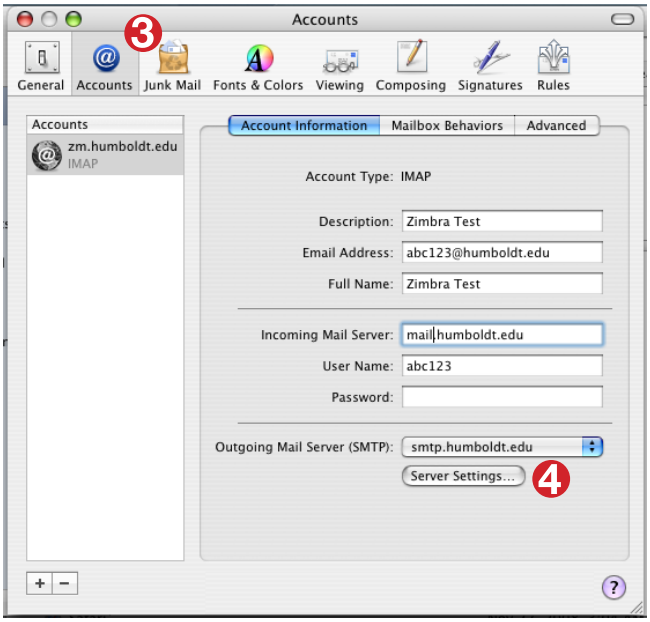
6. Choose **Password** from the **Authentication** pull-down menu. Type your HSU Username and Password in the corresponding fields. Click the **OK** button.



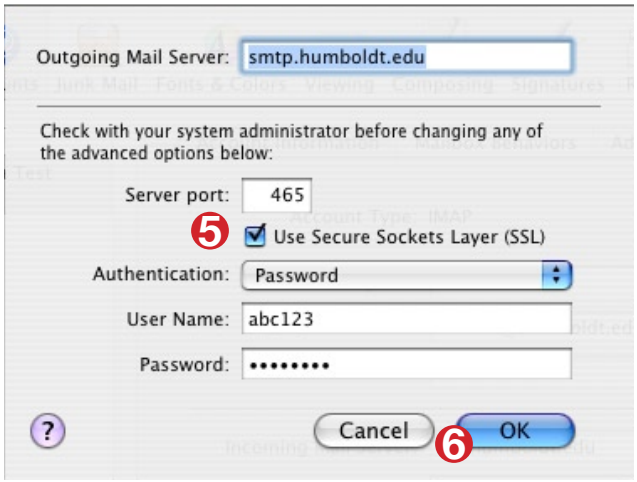
7. Click the **close** button (red button). You will be asked to save your settings. Press the **Save** button.



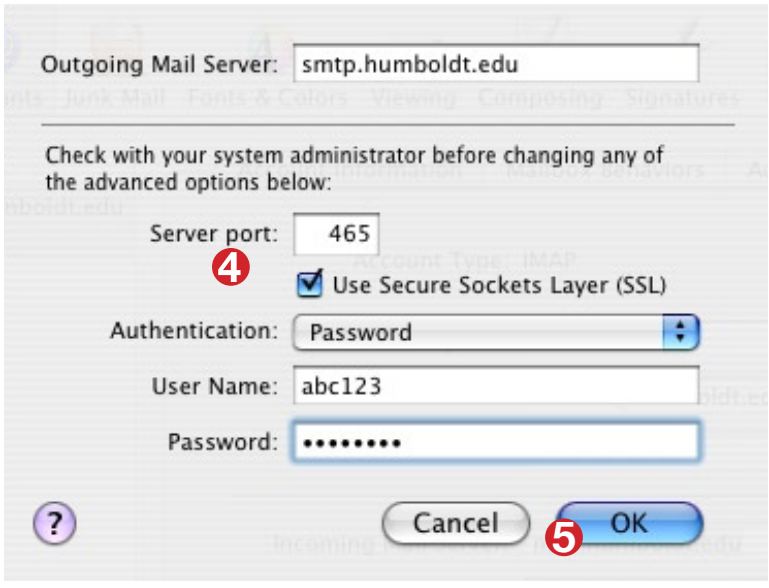
Macintosh Mail (Mac OS X 10.4)



1. Launch Apple Mail
2. In the **Mail** pull-down menu select **Preferences…**
3. Click the **Accounts** category.
4. Click the **Server Settings…** button in the Outgoing Mail Server (SMTP) area.
5. Click the **Use Secure Sockets Layer (SSL)** checkbox. Set the server port to **465**. Choose **Password** from the **Authentication** pull down. Type your HSU Username and Password in the corresponding fields.
6. Click the **OK** button.
7. Click the **Close** button (red button). You will be asked to save your settings.
8. Click the **Save** button.



Eudora for Macintosh*

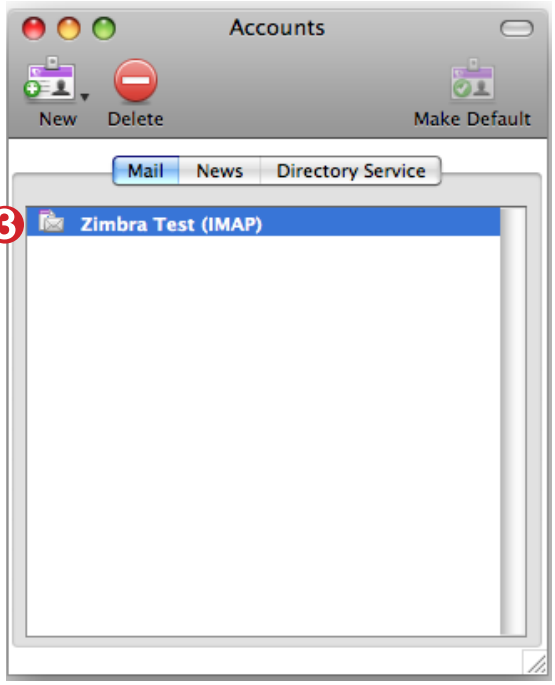


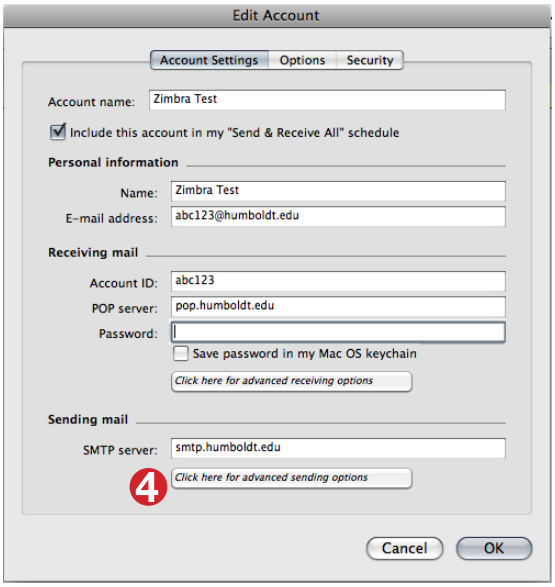
1. Launch Eudora for Macintosh.
2. In the **Eudora** pull-down menu, select **Preferences**…
3. Select the **SSL category.**
4. In the **SSL for SMTP** pull down, select **Required (Alternate Port).**
5. Click the **OK** button.

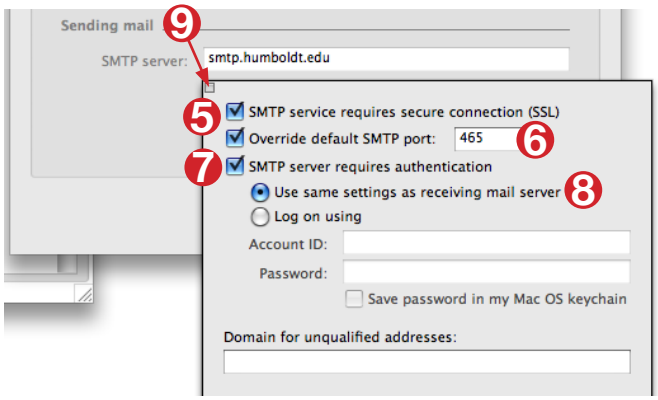
**This software has been removed from our Supported Clients list because of the limited functionality (no calendar support, no synced address books, no shared address books). After this project, we will not be providing instructions for this software.*

Microsoft Entourage 2004/2008*

1. Launch Microsoft Entourage 2008
2. In the **Entourage** pull-down menu, select **Account Settings…**
3. Double-click the account you want to modify.
4. In the Sending Mail section, click the **Click here for advanced sending options** button.
5. Select the checkbox **SMTP service requires secure connection (SSL).**
6. Select the checkbox **Override default SMTP port to 465.**
7. Select the checkbox **SMTP server requires authentication.**
8. Click the **Use same settings as receiving mail server** radio button.
9. Close this window by clicking the little box in the upper left-hand corner.
10. Click the **OK** button in the **Edit Account** window.
11. Close the **Accounts** window using the red button in the upper left-hand corner.



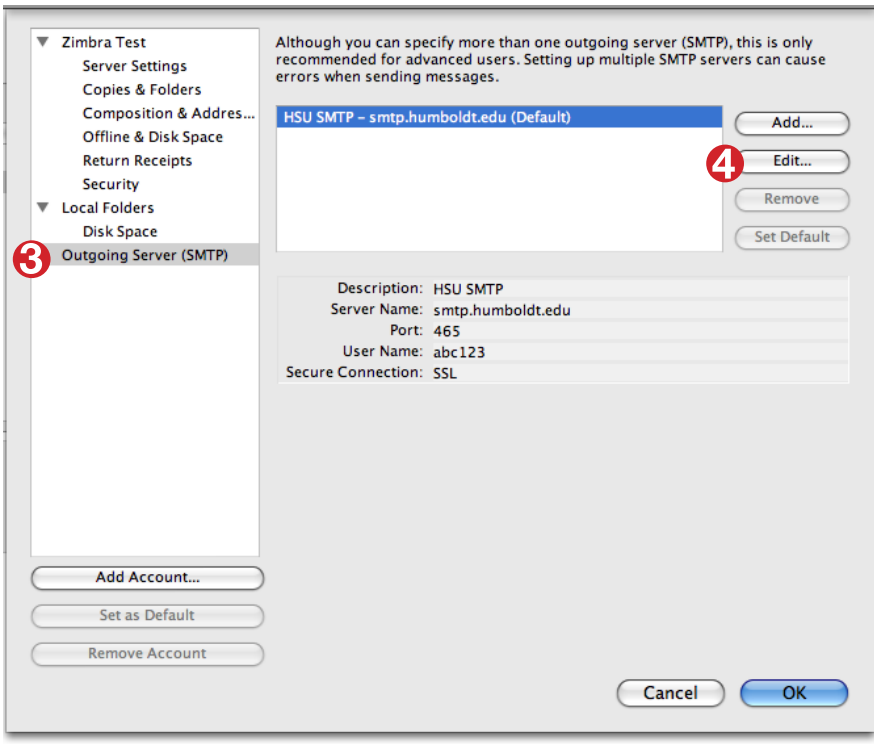




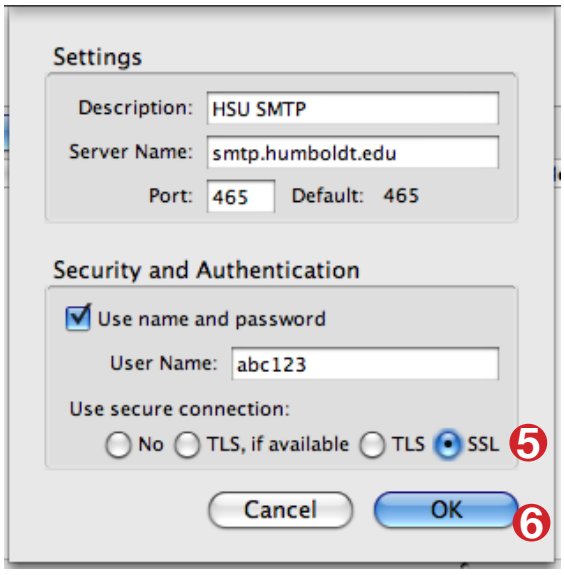
**This software has been removed from our Supported Clients list because of the limited functionality (no calendar support, no synced address books, no shared address books). After this project, we will not be providing instructions for this software.*

Mozilla Thunderbird - Macintosh*

1. Launch Mozilla Thunderbird for Macintosh
2. In the **Tools** pull-down menu, select **Account Settings…**
3. In the left-hand panel select **Outgoing Server (SMTP).**
4. Click the **Edit...** button
5. Select the **SSL** radio button in the **Security and Authentication** section
6. Click the **OK** button for the **SMTP Server** window.
7. Click the **OK** button for the **Account Settings** window.



**This software has been removed from our Supported Clients list because of the limited functionality (no calendar support, no synced address books, no shared address books). After this project, we will not be providing instructions for this software.*



Secure SMTP Migration

Beginning in Fall, 2009, all email clients (including those on-campus) must be configured to use Secure SMTP (the protocol that allows you to transmit email) over port 465 (the standard SSL port) with authentication (a user name and password). This migration continues the Secure Communication project that was started in 2005.

The following settings will be enforced as of October 18, 2009 (off-campus) and April 18, 2010 (on-campus):

- Port 465
- Use SSL
- Use Password Authentication

The settings are available NOW, so you can start making this change anytime.

Why are we making this change to Secure SMTP?

As part of the Secure Communication project in 2005, our email clients were configured to use secure communication methods (encryption) for receiving mail. Off-campus mail users were required to use a secure port (587) for sending mail as well. Until now, on-campus users were able to send mail using port 25, which does not encrypt the connection.

With this change, email clients will be configured the same regardless of being located off-campus or on-campus. This will help reduce confusing instructions, as well as simplify configuration for those who travel with a laptop.

Port 587 will no longer be allowed as it is a non-standard SSL port. The use of this port requires additional configuration on the server that will eventually be unsupported. This change allows us to move to a standards-based configuration.

Port 25 will no longer be allowed because it could allow an unauthorized person to use our system. Using port 465 with authentication ensures that only those who sign in to our system are sending mail on our servers.

Who needs to make these changes?

Zimbra and Outlook (with Zimbra) users

If you are using the Zimbra WebClient (webmail) or Outlook with the Zimbra Connector, you do NOT need to do anything. <Insert instructions for how to tell if Zimbra Connector for Outlook is being used>

Other email clients

If you are using another client (Eudora, Thunderbird, Mac Mail, Entourage, or Outlook without the Zimbra Connector), you will need to make a small configuration change to the way your email client sends mail.

Scripted Process for Mail Sending

If you use a scripted process on a server to send mail, you will also need to adjust your settings. If that is not possible because of the service you are using, you will be required to register that server as a mail sender and continue using port 25. Any unregistered servers will not be able to send mail over port 25 after April 18, 2010.

When do I need to make these changes?

10/18/09: off-campus users will need to have their settings changed to use these new settings.

4/18/10: on-campus users will need to have their settings changed to use these new settings.

Configuration Instructions

Instructions for the following clients are available.

Supported Clients:

- Zimbra WebClient (No configuration necessary)
- Outlook - using the Zimbra Connector (No configuration necessary)
- Outlook - using IMAP or POP instead of the Zimbra connector for Outlook
- Mac Mail

No Longer Supported Clients (Not Recommended):

Please note that the clients listed here were previously supported by the Help Desk and other IT staff. Because of their limited functionality (no calendar support, no synced address books, no shared address books), they have been removed from our Supported Clients list. **After this project, we will not be providing instructions for these clients.**

- Eudora (Windows)
- Thunderbird (Windows)
- Entourage (Mac)
- Eudora (Mac)
- Thunderbird (Mac)

Web Server Migration

Information Technology Services is retiring the aging Sorrel Web server and deploying a pair of new Web servers. The new servers will better focus Humboldt State's communications with its external audiences by enhancing the University's web presence with the latest versions of front-end web technology.

Two new Web servers will replace Sorrel (the campus Web server), the Central HSU Web server and the User Web.

Central HSU Web server (www.humboldt.edu)

The Central HSU Web server hosts all official Department/Official University/Club Sites. The new server is for projects, departmental websites, and initiatives that aid in the positive reinforcement of the University to outside constituents, and facilitate the recruitment of students, staff, faculty, and donors.

User Web (users.humboldt.edu)

The second new Web server is the User Web, hosting all individual non-official accounts.

What Will Be Available on the New Web Servers

New Software Versions

The following will be installed on the new Web servers

- Apache 2.2
- MySQL 5
- PHP 5

Drupal 6

Drupal6 will be available (and managed centrally) on the Central HSU Web server to those who request it.

New Tools

A suite of supported tools will be made available on the Central HSU Web server, to provide services such as form processing and hit counters.

Nicer URLs

The new Web servers will feature nicer URLs. The tilde (~) will be eliminated, making it easier to communicate URLs verbally.

Secure FTP (SFTP)

Secure FTP (SFTP) is FTP over a SSH (Secure Shell) connection where all transferred data is fully encrypted

A Distinction Between "Official" University Accounts and "Individual" Accounts

One of the new Web servers is the Central HSU Web server (www.humboldt.edu), hosting all official Department/Official University/Club Sites.

The second new Web server is the User Web (users.humboldt.edu), hosting all individual non-official accounts.

What Won't Be Available on the New Web Servers

Tildes

The tilde (~) is no longer available on the new Web servers. This will result in cleaner web addresses, which will be easier to write by hand or communicate verbally. Tildes are unintuitive and often cited incorrectly in print.

Tildes used on past web sites will work for two years on the new server.

FTP Access

Traditional FTP (File Transfer Protocol) is insecure and not supported on the new Web servers, as the files being transferred are not encrypted in any way, sending usernames and passwords in clear text. Instead, SFTP is supported. Secure FTP (SFTP) is FTP over a SSH (Secure Shell) connection where all transferred data is fully encrypted. Most organizations have removed support for standard FTP and now only use Secure File Transfer Protocol.

Custom user CGI scripts & Perl

CGI (Common Gateway Interface) is a common scripting method used on web servers. HSU will not support CGI scripts, including perl, on web servers due to the relatively open nature of CGI scripts and the potential to compromise the overall security of the web server. CGI scripts are vulnerable to a large number of exploits that may be used to compromise the overall security of the web server. They are often vulnerable to remote execution exploits, primarily due to inconsistency of coding practices. Also, CGI can impair server performance, as an additional process is started every time the CGI routine is called. This uses memory and other resources on the Web server, which can cause slow response time.

A suite of supported tools will be made available on the Central HSU Web server to provide services such as form processing and hit counters.

SMB access – Mapped Drives (Central HSU Web server)

Server Message Block (SMB) access, which is used for file sharing, can reveal security information and can be an opening for hacks and attacks. If an attacker manages to compromise a Web server, he or she may be able to utilize SMB to further explore and exploit the host network. Personal storage space is available through HSU's Network Folders (www.humboldt.edu/folders). Staff and faculty can utilize mapped shares for file storage. Departmental file shares are a service offered by ITS. *(more information forthcoming)*

Shell access

Providing shell access to a server (logging onto the command line) is a huge security risk. In the interests of security and the protection of our server hardware and software, shell accounts are not available.

What help will be available:

ATI (accessibility) training

The Accessible Technology Initiative (ATI) is an initiative from the Chancellor's Office to make HSU's information technology accessible to all students, faculty, staff and the general public regardless of disability. ATI training will be required for HSU web developers.

Services for making your website ATI compliant are available through the University Web Office and Marketing & Communications. The Web Office provides free consultation for website redesigns and updates, and will also make available ATI and University style guide compliant templates for your website. For information about these solutions contact Marketing & Communications at 826-3321 or webmaster@humboldt.edu.

File migration support

Information, such as connection details for Dreamweaver and SFTP applications, will be provided for migrating your files from the old web server to the new web server. When you have moved your site and are ready, there is a tool that will automatically redirect visitors from your old site to the new one.

For personal web pages (User Web), your files can be moved for you. This tool will be available in Account Center after August 1, 2009. After your files are moved (with this tool), visitors to your old site will automatically be redirected to the new one (for how long?).

Who will have accounts on the new web servers:

Individuals (students, staff and faculty)

User Web (users.humboldt.edu) will host all individual non-official accounts

Departments (site owners and developers)

Central HSU Web server (www.humboldt.edu) will host all official Department/Official University/Club Sites

Why is this change being made:

Aging equipment

HSU's Sorrel Web server is in need of an upgrade. The new server will provide performance gains and will better focus Humboldt State's communications with its external audiences by enhancing the University's web presence with the latest versions of front-end web technology.

Accessiblity (ATI)

The ubiquity of the Internet in delivering information and providing services is an essential reason to make its accessibility a priority for the CSU. Creating and maintaining accessible websites will be an ongoing institutional responsibility. The dynamic nature of the web and the continuous updating of content require a process that can be facilitated by the use of an enterprise-wide web evaluation and monitoring tool along with well-defined campus policy and implementation procedures.

When is this taking place?

Announcements about the Web server change: Ongoing April through next Fall 2009

Early Adopters: Summer 2009

Central HSU Web server: 8/1/09 – Fall/Early Spring 2010 (9 month migration)

User Web: 8/1/09 – Fall/Early Spring 2010

Tildes will work for 2 years from the go-live of the new Web server. Please update any documents (printed and/or electronic) that may have your old address listed.

How to activate accounts on the Central HSU Web server after 8/1/09 (www.humboldt.edu):

Departmental accounts will be activated with the following steps:

1. A new site will be requested (along with a new "nice" name, approved by the Web office). No tildes (~) will be used.

2. Site owners must complete Accessibility Training. This is accomplished by logging onto Account Center and sign up for ATI training.

3. Site owners designate site developers. If the site owner is not doing the development themselves, they can designate a separate developer.

4. Site owners and developers must complete Accessibility Training.

5. Sites will become activated once training has been completed .

6. Developers will gain access to a site's files by logging into the server with his or her own HSU User Name. A developer will have access to any site(s) for which he or she is listed as a developer.

7. The developer will do any work necessary to make the site ATI compliant, ensure compatibility with upgraded MySQL and PHP versions, and move files over to the new server.

8. After ATI compliance verification, the Developer or Owner can request to make the site "live" so any attempts to reach the "old" address will be directed to the new site.

9. Once the site is live, a visit to www.humboldt.edu/~oldsite would display a page that informs the visitor that the site has been moved to www.humboldt.edu/newsite

How to activate accounts on the User Web after 8/1/09(users.humboldt.edu):

Users will activate their accounts with the following steps:

1. Complete an ATI survey. This is accomplished by logging into Account Center (formerly known as WebReg).
2. Select an alias (for URL display and email)
3. Optionally, move the old web site automatically