Next Steps.

Congratulations! You've successfully set up Mac OS X Server, the world's easiest-to-use server operating system, and you're now ready to use many of the exciting services that it has to offer. To enhance the security, accessibility, and overall usefulness of your new server, there are a few additional changes you should make to your network, and this document will help you get started. These items may require changes to components of your network such as routers and other servers. If you don't have access to these components, contact the person who's responsible for them.

Users and Groups

Some of the services running on your server require users to enter a user name and password to access them. Use the Users pane and Groups pane of Server Preferences to create accounts and manage the users and groups who access your server. For detailed instructions, search Server Preferences Help for "managing accounts."

Certain tools for managing your users, groups, and other resources, such as Workgroup Manager and iCal Server Utility, enable you to log in using your directory administrator. Your directory administrator has the user name "diradmin", and its password is the same as the admin user you created during setup.

Port Forwarding

Your server is connected to the Internet through a NAT device, such as a network router, which may prevent some users who are outside your immediate network from accessing services. If you don't want to provide access to users outside your immediate network, you can skip this step.

To allow access to all users, including those outside your immediate network, you need to configure port forwarding on your NAT device. To do this, use your device's configuration software, which usually consists of several webpages at an address such as http://192.168.1.1 or http://192.168.1.254. Using Safari, you go to the configuration website, and then navigate to the webpage with settings for "Port Range Forwarding," "Port Mapping," "Firewall Settings," or "Virtual Server." In some cases, you can select standard services such as web or VPN and specify that each be forwarded to your server's IP address. In other cases, you must enter port numbers for services and enter your server's IP address for each one. For specific information about configuring your NAT device, see its documentation.

The ports to forward for many of your services are listed below. Some NAT devices may ask you to specify TCP or UDP for each port, while other devices don't. For a list of ports for additional services, search Server Admin help for "TCP and UDP port reference," or see http://support.apple.com/kb/TS1629

Description	Ports	Protocols
Apple File Service (AFP)	548	TCP
ARD – Remote Management	3283, 5900	TCP, UDP
HTTP – web service	80	TCP
HTTP – web service alternate	8080	TCP
HTTPS – secure web service via SSL	443	TCP
iCal Server	8008	TCP
iCal Server – SSL	8443	TCP
iChat Server	5222	TCP
iChat Server – file transfer proxy	7777	TCP
iChat Server – server-to-server	5269	TCP
iChat Server – SSL	5223	TCP
Mail – IMAP	143	TCP
Mail – IMAP SSL	993	TCP
Mail – POP3	110	TCP, UDP
Mail – POP3 SSL	995	TCP, UDP
Mail – SMTP legacy SSL submission	465	TCP
Mail – SMTP standard	25	TCP, UDP
Mail – SMTP submission	587	TCP
SMB/CIFS – Windows file service	161	TCP
SSH – Secure Shell	22	TCP, UDP

Configure DNS

The domain name servers you're using don't have an entry for the name demo.tooltwist.com, and therefore your clients won't be able to access your server using this name. If your organization has its own DNS servers, ask your IT department to add a DNS entry for demo.tooltwist.com that resolves to the address your server. If your organization doesn't have its own DNS servers, add this entry through your ISP or with the public domain name registrar where your domain is registered.

If your server only needs to be accessed by clients on the your local network (IP subnet), your server can provide the necessary domain name resolution. In order for your clients to use your server for name resolution, you need to configure your server's DNS service to provide DNS forwarding, and then configure your DHCP server (usually your network router) to provide your server address (10.0.1.167) as the primary DNS server. To configure DNS forwarding, make a note of the DNS servers that are currently being used by your router or DHCP server. Open Server Admin, connect to your server, select DNS service, click Settings, and then add those DNS servers to the Forwarder IP Addresses list. For information about how to change the DNS servers that your router or DHCP server provides to clients, see the manual for your device.

Create a Signed SSL Certificate

The server can use an SSL certificate to identify itself electronically and securely communicate with users' computers and other servers on the local network and the Internet. The SSL certificate provides additional security for address book, iCal, iChat, mail, and web services. These services can use the certificate to securely encrypt and decrypt data they send to and receive from applications on users' computers.

You can use the self-signed certificate created for your server when you set it up, or a self-signed certificate you created, but users' applications won't automatically trust it and will display messages asking if the user trusts your certificate. Using a signed certificate relieves users from the uncertainty and tedium of manually accepting your certificate in these messages. In addition, a man-in-the-middle spoofing attack is possible with a self-signed certificate, but not with a signed certificate, and that means users can trust the services they are accessing.

To use a self-signed certificate, open the Information pane in Server Preferences, click the Edit button to the right of SSL Certificate, select "Use SSL certificate," and then choose an available certificate from the top part of the pop-up menu. For more information, search Server Preferences Help for "using an SSL certificate."

You can obtain a valid signed certificate by using the server's self-signed certificate to generate a certificate signing request (CSR) file, which you send to a known certificate authority. If your request satisfies the authority, it makes a signed certificate and sends it to you.

To obtain a signed certificate, open the Information pane in Server Preferences, click the Edit button to the right of SSL Certificate, and choose the self-signed certificate you want to use from the pop-up menu. Then choose Certificate Signing > Generate Certificate Signing Request from the pop-up menu, click Save, and choose a location to save the certificate signing request (CSR) file. Send the contents of the CSR file to a certificate authority—typically you paste the contents of the CSR file into a form on the certificate authority's website.

Here are a few certificate authorities:

- Thawte, Inc. (www.thawte.com)
- VeriSign, Inc. (www.verisign.com)
- Comodo, Inc. (www.comodo.com)

After receiving your signed certificate from the certificate authority, you can use it to replace your self-signed certificate. First, put the file somewhere you'll be able to see it while using Server Preferences. Then open the Information pane in Server Preferences, click the Edit button to the right of SSL Certificate, and choose the self-signed certificate you want to replace from the pop-up menu. Choose Certificate Signing > "Replace With Signed or Renewed Certificate."