



Administration Guide

Note

Before using this information and the product it supports, read the information in "Notices" on page 157.

This edition applies to version 1.1, release 1 of IBM Lotus Foundations (product number 5724-V16) and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright International Business Machines Corporation 2009.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

Lotus Foundations Start Administration Guide 1

| | |
|---|----|
| Introduction | 1 |
| First-time Lotus Foundations setup on a Lotus Foundations Appliance | 1 |
| Connecting to the Internet - Ethernet ports 1 and 2 | 1 |
| Connecting an external dial-up modem | 2 |
| First-time Lotus Foundations setup on third-party hardware | 3 |
| Connecting to WebConfig | 3 |
| What is WebConfig? | 3 |
| Secure WebConfig | 4 |
| Configuring TCP/IP | 4 |
| Creating an administrator account | 6 |
| Software activation keys | 8 |
| System status screen | 9 |
| Notices box | 13 |
| System status details | 13 |
| Installing the Lotus Foundations Start add-on | 14 |
| Lotus Foundations Start introduction | 14 |
| Lotus Foundations Start installation | 15 |
| Execution control list (ECL) alerts | 15 |
| Configuring Lotus Foundations | 16 |
| Proceeding with configuration | 16 |
| Configuring General Network Settings | 16 |
| Configuring advanced DHCP settings | 18 |
| Configuring advanced network settings | 19 |
| Network devices | 19 |
| Network routes | 20 |
| Network configuration scenarios | 21 |
| Configuring your internet connection | 23 |
| User licenses | 25 |
| User licensing requirements | 25 |
| License information | 25 |
| DoubleVision | 26 |
| What is DoubleVision? | 26 |
| What DoubleVision offers | 26 |
| Modem connections | 27 |
| How internet failover and DoubleVision work | 27 |
| User & Team management | 29 |
| Service integration | 29 |
| User accounts | 30 |
| Modifying user email settings | 33 |
| Team accounts | 33 |
| Password policy | 35 |
| File services | 36 |
| File sharing services | 36 |
| Configuring file services | 37 |
| Active server connections | 38 |
| Access control lists | 38 |
| Setting permissions in Windows | 39 |
| Disk quotas | 40 |
| Setting default disk quota values | 40 |
| Setting individual user disk quotas | 40 |
| Quota limit | 41 |

| | |
|--|----|
| NT domain services | 41 |
| Configuring Lotus Foundations Domain Settings | 41 |
| What is a domain controller? | 42 |
| Configuring the domain controller | 42 |
| What is a Windows NT domain member? | 43 |
| Configuring the domain member | 43 |
| Connecting the active directory member | 43 |
| Verifying server connectivity | 44 |
| Monitoring machine accounts | 44 |
| Importing domain users and groups | 45 |
| File mounting/drive mapping | 46 |
| Joining Windows systems to a domain | 46 |
| Logon scripts | 48 |
| Automated drive mapping | 48 |
| Workstation administrative rights | 48 |
| Lotus Foundations scalable services | 48 |
| Lotus Foundations scalable services terminology | 49 |
| Features of Lotus Foundations scalable services | 49 |
| Lotus Foundations scalable services regions | 51 |
| Setting up a scalable services region | 53 |
| Lotus Foundations scalable services frequently asked questions | 59 |
| Print service | 59 |
| Lotus Foundation print services | 59 |
| Configuring local print services | 60 |
| Configuring your workstation | 60 |
| Other network printing | 60 |
| Performing printing queue tasks | 61 |
| Email services | 61 |
| Configuring email services | 61 |
| Features handled by IBM Lotus Domino | 62 |
| Email DNS configuration | 68 |
| Email client configuration | 69 |
| Using Lotus Domino email clients | 71 |
| Installing the Lotus Domino Access for Microsoft Outlook (DAMO) add-on | 71 |
| Web services | 73 |
| Web server | 73 |
| Master Web server | 73 |
| Virtual Web servers | 76 |
| Hosting multiple Web sites | 78 |
| Secure Web services | 79 |
| SSL certificate | 79 |
| Web caching | 80 |
| Web filtering | 80 |
| Web and content filtering | 80 |
| Enabling the Web filter | 80 |
| Providing full internet access | 80 |
| Port exemptions | 81 |
| Adding permitted Websites | 81 |
| Adding denied Websites | 81 |
| Accepting access requests | 81 |
| Denying access requests | 82 |
| List management | 82 |
| Email reporting | 83 |
| FTP services | 83 |

| | | | |
|---|-----|---|-----|
| FTP Server | 83 | Recovering from disk failure | 113 |
| Anonymous FTP Server | 83 | Hard disk failure | 113 |
| Enabling the FTP server | 83 | Installing a new hard drive | 114 |
| Enabling FTP access for a specific team or user | 84 | Backup & Restore | 114 |
| User vs. Team FTP access. | 84 | Intelligent disk backup (idb) | 114 |
| Software update | 85 | Configuring idb | 115 |
| Upgrading Lotus Foundations | 85 | idb backup | 119 |
| Switching languages | 86 | idb restoration | 121 |
| Virtual private networks | 86 | Lotus Domino restoration procedures | 124 |
| Private networks | 86 | idb hot swap | 126 |
| Virtual private networks | 87 | MySQL server | 127 |
| VPN network topologies | 88 | What is the MySQL Server? | 127 |
| How TunnelVision works. | 89 | Setting up Windows for MySQL Access | 127 |
| Creating a VPN (server-to-server) | 90 | What is a dynamic Web site? | 128 |
| Configuring a TunnelVision master server | 91 | Hardware components reporting | 128 |
| Configuring a TunnelVision client | 92 | Log messages | 129 |
| TunnelVision status. | 92 | Accessing log messages | 129 |
| The idle time-out | 93 | Customizing message display | 129 |
| IPsec | 93 | Firewall log | 129 |
| Known configurations | 93 | Network file system | 130 |
| Adding an IPsec route. | 93 | What is NFS? | 130 |
| Adding an anonymous incoming connection | 93 | rsync | 131 |
| IPsec route | 94 | What is rsync? | 131 |
| Editing an IPsec route | 94 | Enabling rsync | 131 |
| Setting up third-party IPsec clients | 95 | rsync from a Telnet session | 132 |
| Remote access services | 95 | Lotus Foundations Run feature | 132 |
| What is RAS?. | 95 | Installing the Lotus Foundations Run 1.1 add-on | 133 |
| PPTP - client-to-server VPN service | 96 | Using the VMware server | 135 |
| Dial-in service | 98 | Editing Lotus Foundation Run add-on settings | 136 |
| Terminating a connection from WebConfig | 99 | Backing up and restoring the virtual machine | 138 |
| Firewall services | 99 | Troubleshooting | 138 |
| Traffic denied inbound | 99 | Lotus Symphony | 139 |
| Traffic permitted inbound | 99 | How does Symphony compare to other similar offerings?. | 139 |
| Traffic permitted outbound | 99 | Installing Lotus Symphony add-on to the server | 139 |
| Firewall log | 101 | Installing Lotus Symphony to client workstations. | 140 |
| Domain Name Service | 101 | Switching between languages | 141 |
| What is DNS? | 101 | Spam scanner | 142 |
| DNS Services | 101 | Installing the Lotus Foundations anti-spam network filtering feature. | 142 |
| Configuring Public DNS. | 102 | Activating your spam scanner | 143 |
| How the DNS system works | 102 | Configuring users' spam filters | 143 |
| Dynamic DNS | 103 | Virus scanner | 144 |
| Manually creating DNS entries | 103 | Activating your file virus scanner license | 144 |
| Workstation viewer | 104 | Activating your mail virus scanner license. | 145 |
| What is the workstation viewer? | 104 | Lotus Foundations Start performance optimization | 147 |
| Accessing the workstation viewer | 104 | Minimum hardware requirements | 147 |
| Virtual network computing (VNC) | 105 | Quick reference and hardware sizing guide | 147 |
| Configuring VNC | 105 | Email protocol choices affecting server performance. | 148 |
| Fast/Port Forward | 106 | Other services running on the Foundations Server. | 148 |
| What is Fast/Port Forward? | 106 | Backup scheduling | 149 |
| Introduction to TCP/IP | 106 | Future capacity planning | 149 |
| Proxy servers | 107 | Glossary | 150 |
| Configuring Fast/Port Forward | 107 | Notices 157 | |
| Forwarding scenarios. | 109 | Trademarks | 158 |
| Multiple static IP addresses. | 109 | | |
| Common port numbers | 110 | | |
| Troubleshooting Fast/Port Forward | 110 | | |
| Disk management | 110 | | |
| Disk configuration (idb and RAID) | 110 | | |
| Reconfiguring your disks | 111 | | |
| Disk status messages | 112 | | |

Lotus Foundations Start Administration Guide

Introduction

Welcome to the *Lotus® Foundations Start Administration Guide*. This document is intended for administrators and provides the instructions required to install a completely functional Lotus Foundations Start server. In addition, a description of core Lotus Foundations features are included to provide you with an understanding of the Lotus Foundations Start server overall.

First-time Lotus Foundations setup on a Lotus Foundations Appliance

See the *Lotus Foundations Start Getting Started Guide* for instructions on the general setup of the Lotus Foundations Appliance. Advanced and less common configurations are included in this guide.

Connecting to the Internet - Ethernet ports 1 and 2

Ethernet ports 1 and 2 are used to connect to the Internet or to other segments of your local area network (LAN). Use an Ethernet cable to connect to your high-speed Internet routing device. Some devices might require the use of a crossover cable that is normally supplied with the device.



Figure 1. View of Ethernet ports 1 and 2

The figure above displays the locations of Ethernet ports 1 and 2:

1. Ethernet port 1
2. Ethernet port 2

If you are using your Lotus Foundations Appliance as a workgroup server without a direct connection to the Internet, it is possible to use Ethernet ports 1 and 2 to connect to other segments of the LAN. This is typically done to improve network throughput when large numbers of users are connected to Lotus Foundations.

Secondary segments must be physically separate from the primary network segment connected to the Ethernet port 0. You cannot connect all Ethernet ports to the same segment to improve network throughput.

Connecting an external dial-up modem

1. Connect the cable included with your own external dial-up modem to the serial port on the back of the Lotus Foundations Appliance.
2. Connect one end of the standard telephone cable to the external modem, and connect the other end to your telephone wall jack.

The external modem is auto-detected when the server goes through a power-up sequence.

First-time Lotus Foundations setup on third-party hardware

Lotus Foundations has built-in diagnostics to help you determine hardware compatibility. The following are third-party hardware requirements:

- x86 based system
- At least one hard disk. At least two hard drives are needed to back up your data.
- At least one Network Interface Card. Two network cards are needed if this is your network gateway.
- DVD drive
- VGA based video card
- 1 GB RAM
- Monitor
- Keyboard

Your third-party hardware must be free of any other applications, files, or operating environment. It is recommended that a new disk be used. It is strongly recommended that you also have your hardware-specific reference documentation. Lotus Foundations Start first installs the base operating system and overwrites any data on the disk drive. The setup process also configures the disk drives.

Before you begin installing on the third-party hardware you need to change the system BIOS to ensure you are able to boot from DVD. Do this through the boot settings in system BIOS. Change the boot priority order to the following:

- First boot device: CD (or DVD)
- Second boot device: hard disk drive

Lotus Foundations installs onto the hard disks after they have been configured.

Connecting to WebConfig

What is WebConfig?

Lotus Foundations administrators use WebConfig to assign required and optional settings for the environment. Administrators access WebConfig through an Internet browser connected to the local network. This section provides user guidance for WebConfig. For instructions on how to access WebConfig, see “Creating an administrator account” on page 6.

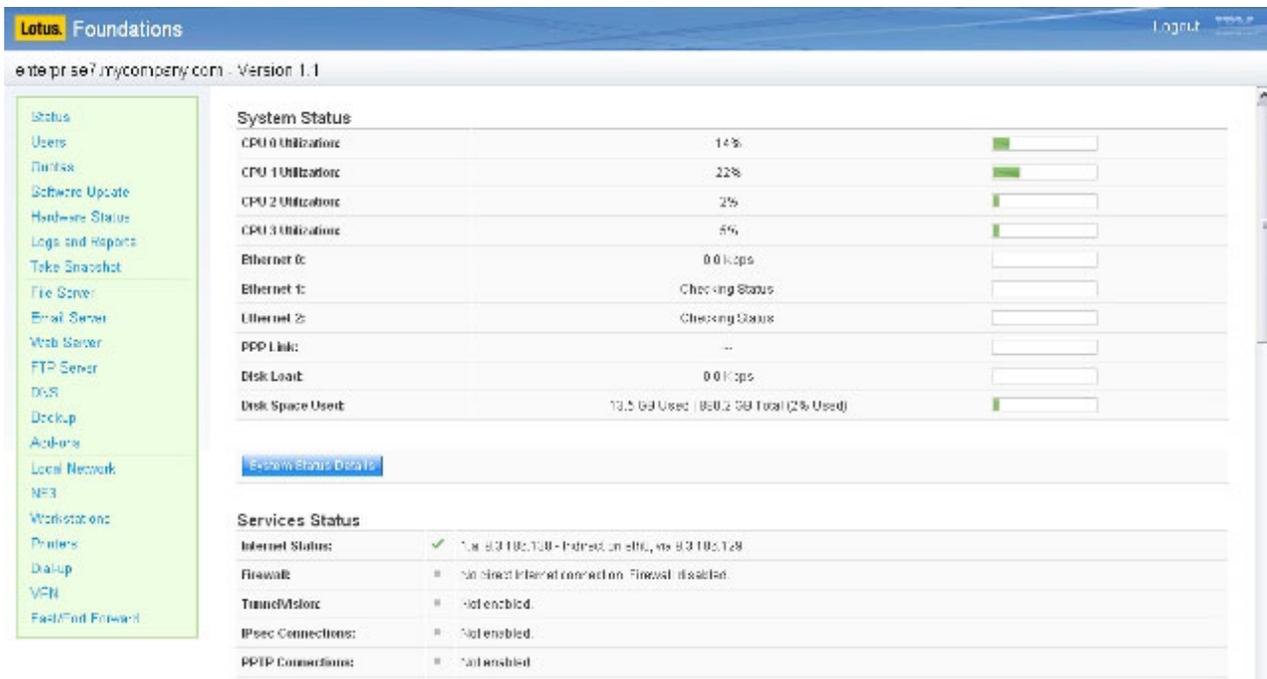


Figure 2. The main screen of WebConfig

Secure WebConfig

Lotus Foundations' WebConfig uses 128-bit encryption to protect administrator information and passwords. Most recent versions of Web browsers contain built-in support for this. Lotus Foundations WebConfig supports these web browsers:

- Internet Explorer 6 and any later versions.
- Firefox 1.0.5 and any later versions.

WebConfig is unreachable if there is a failure to support 128-bit encryption results.

Other Web browsers that might work but are not explicitly supported are:

- Opera
- Safari
- Netscape
- Mozilla

Configuring TCP/IP

Before you can access WebConfig, you have to configure your workstation to use TCP/IP. If TCP/IP is already configured, proceed to "Creating an administrator account" on page 6. If TCP/IP is not configured, follow the appropriate steps for your operating system.

For Windows® 95/98/ME:

1. In Windows, select **Start** → **Settings** → **Control Panel**. The Control Panel window is displayed.
2. Select **Network** from the list. The Network window is displayed. Click **Add** if TCP/IP is not displayed in the installed components list.
3. The Select Network Component window is displayed. Select **Protocol** from the window and click **Add**.

4. The Select Network Protocol window is displayed. Select **Microsoft®** in the Manufacturers section of the window. Select **TCP/IP** in the Network Protocols section of the window. Click **OK**. TCP/IP is now displayed in the Network window.
5. Select **TCP/IP** from the installed components list on the Network window. Click **Properties**. The TCP/IP Properties window is displayed.
6. Click the **IP Address** tab. Select **Obtain an IP address automatically**.
7. Click the **DNS** tab. Select **Enable DNS**.
8. Select all entries in the DNS Server Search Order section of the window and click **Remove**.
9. Select all entries in the Domain Suffix Search Order section of the window and click **Remove**.
10. Select **Obtain an IP address automatically**.
11. Click the **Gateway** tab. Select any entries in the Installed gateways section of the window and click **Remove**.
12. Click the **WINS Configuration** tab. Select all entries in the WINS Server Search Order section of the screen and click **Remove**. Select Use DHCP for WINS Resolution.
13. Click **OK**. The Network window is displayed. Click **OK** again.
14. Reboot the computer.

For Windows 2000/XP:

1. In Windows 2000, select **Start → Settings → Control Panel**. On Windows XP, click **Start → Control Panel**. If Windows XP is in Classic mode, the control panel is under **Start → Settings → Control panel**.
2. Select **Network and Dial-up Connections** from the list. The Network Connections screen is displayed. In Windows XP, select **Network and Internet Connections**, then click **Network Connections**.
3. Double-click **Local Area Connection** and the Local Area Connection window is displayed.
4. Click **Properties** and the Local Area Connection Properties window is displayed. If Internet Protocol (TCP/IP) is not in the Components checked that are used by this connection list, click **Install**.
5. The Select Network Component Type is displayed. Select **Protocol** from the window. Click **Add**.
6. The Select Protocol window is displayed.
7. Select **Internet Protocol (TCP/IP)** from the list. Click **OK**. TCP/IP should now be displayed in the Local Area Connection Properties window.
8. Select Internet Protocol (TCP/IP) from the list, and click **Properties**.
9. The Internet Protocol (TCP/IP) Properties screen is displayed. Select **Obtain IP Address automatically**. Select **Obtain DNS server address automatically**.
10. Click **Advanced**. The Advanced TCP/IP Settings window is displayed. Select any entries in the Default gateways section of the window, and click **Remove**.
11. Click the **DNS** tab. Select any entries in the DNS server addresses section of the window, and click **Remove**. Select **Append primary and connection specific DNS suffixes**. Select **Append parent suffixes and primary DNS suffixes**.
12. Click the **WINS** tab. Select any entries in the WINS addresses section of the window, and click **Remove**. Select the Default NetBios setting.
13. Click **OK**. Click **OK** on the TCP/IP Properties screen.
14. Reboot the computer.

For Mac OS 9:

1. Click the Apple icon in the top menu bar. Select **Control Panel → TCP/IP**.
2. The TCP/IP window is displayed.
3. Select **Connect via Ethernet**. Select **Connect via DHCP**. Leave the other fields blank.
4. Click the **Close Window** button. The Save screen is displayed.

5. Click **Save**.
6. If the Internet connection does not function immediately, reboot the computer.

For Mac OS X:

1. Click the Apple icon in the top menu bar. Select **System Preferences**. The System Preferences window is displayed.
2. Click the **Network** icon. The Network screen is displayed.
3. Select **Automatic for location**. Select Built-in Ethernet for connection. In the TCP/IP tab, select the DHCP configuration.
4. Click **Apply Now**.
5. If the Internet connection does not function immediately, reboot the computer.

Creating an administrator account

At this point, the Lotus Foundations server should have an IP address, the workstation should have TCP/IP configured, and both the Lotus Foundations server and the workstation should be connected to the LAN. You now need to create an administrator account.

To create an administrator account, follow these steps:

1. Read the IP address on the server console of the Lotus Foundations server. For demonstration purposes, the IP address 192.168.0.1 is used.
2. Open a Web browser on a workstation, and enter in the IP address for the server, appending port 8043. You must use a secure Web connection using https. For example: <https://192.168.0.1:8043>
3. Select a default language. Read and accept the licenses on the next two screens. The Create Administrator Account page is displayed.

The screenshot shows the 'Create Administrator Account' page in Lotus Foundations. On the left is a circular orange icon with a white building. The page title is 'Create Administrator Account'. Below the title is a note: 'Before you can use your server, you must create an Administrator Account for yourself. The password and domain fields are mandatory.' The form contains the following fields: 'Default Language' (dropdown menu set to 'English'), 'User ID' (text box with 'root'), 'Full Name' (text box with 'System Administrator'), 'Password' (password box with 8 dots), 'Re-enter Password' (password box with 8 dots), 'Your Domain Name' (text box with 'mycompany.com'), and 'Activation Key' (text box with '(leave blank to continue in trial mode)'). At the bottom are two buttons: 'Save Changes' and 'Cancel Changes'.

Figure 3. Creating an administrator account

4. To create an administrator account, leave the user ID as **root**. Enter a valid password, and reenter the password. Write this password down in case you forget it. Caution: the administrator user ID must be **root**. You can create additional administrator accounts later.
5. Enter a domain name. Any domain name can be entered at this point. The organization's real domain name is required before you install Lotus Foundations Start.
6. Enter the Software Activation Key in the Activation Key text box. If you do not have an activation code, the Lotus Foundations continues to function in trial mode for 30 days and you can enter the activation key at any time during that period. During that 30 day period, you can use all of the core features of the product, with the exception of anti-virus and anti-spam protection.
7. Click **Save Changes**. This takes you directly to the Lotus Foundations WebConfig console.
 - Some browsers take you to an Administrator Account Created page. If this occurs, click **Login** and you are taken to the main WebConfig page. Clicking **Cancel Changes** resets the Create Administrator Account form.

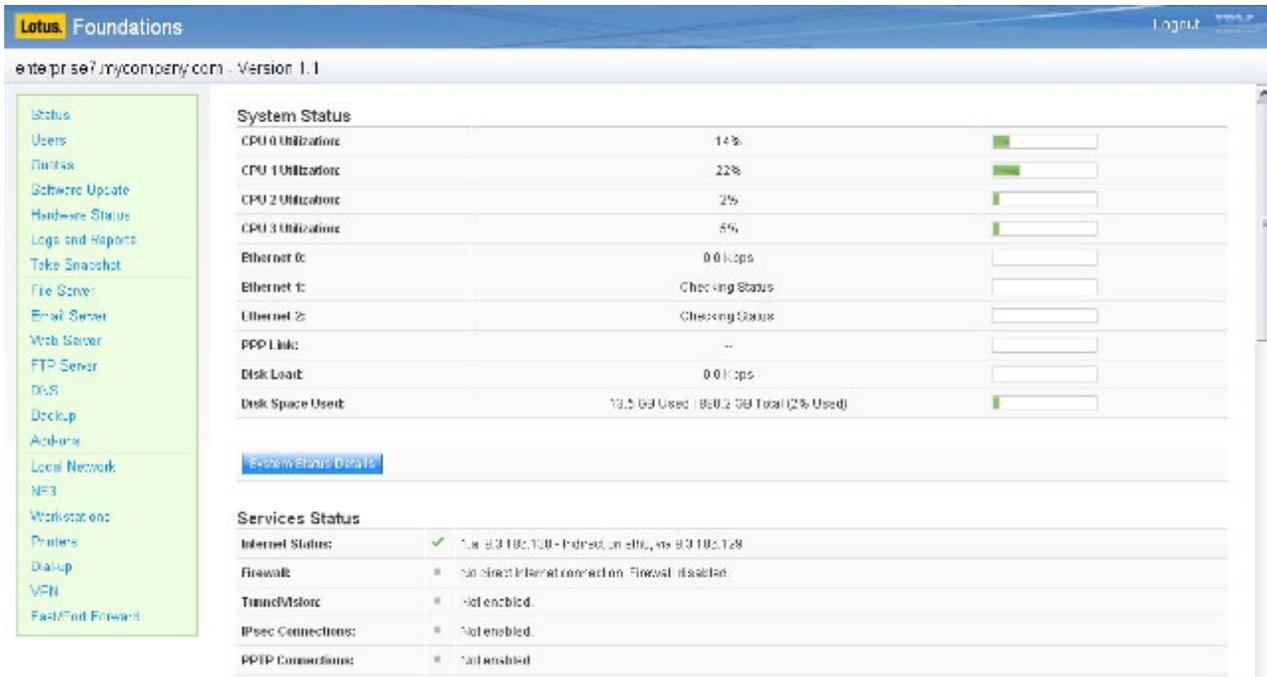


Figure 4. Main Status page of WebConfig

Note: Some Lotus Foundations services are not enabled unless hard disks are configured through WebConfig. For more information on configuring hard disks, see “Disk management” on page 110.

Software activation keys

By default, Lotus Foundations comes configured in a 30-day trial mode. To get out of trial mode and activate the features and licenses you have purchased, you must enter a software activation key.

When you purchase Lotus Foundations software, a software activation key is provided.

Note: An Internet connection is required for activating the Lotus Foundations software license. It is the user’s responsibility to ensure that an Internet connection is established when attempting to install the software.

Enter activation key to exit trial mode

Follow these steps to enter the software activation key:

1. Login to WebConfig with an administrator account.
2. Click **Software Update**.
3. Enter your activation key in the Foundations Registration section.
4. Click **Save Changes**.



Figure 5. Registration section of the Web Configuration console

Updating your activation key

Follow these steps to replace an existing activation key with a new one:

1. Login to WebConfig with an administrator account.
2. Click **Software Update** and you see the current activation key displayed under the Foundations Registration section.
3. Click the Edit action button  and the Lotus Foundations Registration box is displayed.
4. Enter the new activation key in the Lotus Foundations Registration box.
5. Click **Save Changes**.



Figure 6. Editing the activation key in the Web Configuration console

System status screen

The system status screen displays the status of the services running on Lotus Foundations. The WebConfig menu helps you to access and configure various Lotus Foundations subsystems.

Table 1. Features of the system status screen

| Item | Description |
|--|---|
| CPU utilization | Displays the use of the system's central processing unit (CPU) in numerical form and as a bar graph. During intensive operations (such as backups or very heavy file transfers), the CPU use bar might show 100%. This is normal. One hundred per cent use simply means that the CPU is being fully used and does not necessarily mean that your Lotus Foundations server is being overloaded or that performance suffers. However, if the CPU use is constantly at 100%, and you experience service slow-downs, you might want to contact support for a services review. |
| Ethernet 0, Ethernet 1, and Ethernet 2 | Displays the speed of data transfer through Ethernet port 0, port 1, and port 2 (measured in kbps or Mbps). The bar graph displays the speed as a percentage of the highest transfer rate recorded since the last power-up. |

Table 1. Features of the system status screen (continued)

| | |
|------------------------------|--|
| PPP link | Displays the speed of data transfer through the DSL PPPoE or dial-up Internet connection (measured in kbps). The bar graph displays the speed as a percentage of the maximum measured speed. |
| Disk load | Displays the amount of data being transferred to and from the hard disk (measured in kbps or Mbps). The bar graph displays the amount as a percentage of the highest amount recorded since the last power-up. |
| Disk space used | Displays how full your server hard disk is by displaying the usage and capacity of the drive. |
| System status details button | Displays System Status resource information in a graphical representation, on a variable time basis, for example, half hour, 1 month, or 1 year. Also includes graphs for Physical Memory and Virtual Memory. |
| Internet status | Displays the status of your internet connection(s). A green check mark displays when an internet connection is configured properly. The default route used to transfer data to destinations on the internet is also displayed. If a modem is configured, clicking dial modem initiates a connection to the internet. The administrator can choose to terminate the connection through this screen. |
| Firewall | Displays the status of the firewall (enabled/disabled). |
| TunnelVision | Displays the status of all TunnelVision connections. |
| IPsec connections | Displays the status of all IPsec connections. |
| PPTP connections | Displays the status of all PPTP connections and provides an option to disconnect active connections. |
| SoftUpdate | Displays the status of the subsystem that automatically checks for available software updates. When the subsystem is active and retrieving a list of available software updates, the status light is green. When the subsystem is operational but idle, the status light is gray. A red status light indicates a problem with the subsystem (usually an inability to access the distribution server). Refer to "Log messages" on page 129 for more information on download errors. |
| Disk status | Displays the status of your disk configuration, provides disk reconfiguration options, displays the status of a rebuilding RAID array, and displays idb drive hotswap status. |
| Backup status | Displays the status of the idb backup disk. It displays how much of the idb disk space is currently available for backups and when the next backup is scheduled to be done. |
| Quota status | Displays if there are any users over their quota limit. See "Setting individual user disk quotas" on page 40 for more information. |
| Scalable services status | Displays the status of the Scalable Services Structure. |

Table 1. Features of the system status screen (continued)

| | |
|----------------------------|---|
| Add-ons | Displays the status of any Lotus Foundations add-ons running on the Lotus Foundations server. In Lotus Foundations Start, Domino® specific information is displayed, such as the status of the Domino server's 'listener' and the status of the NDC support services (next and last backup time and the next and last database compression time). |
| User authentication method | Displays the method of authentication currently enabled. It displays "Using normal password authentication" if Lotus Foundations is in Domain Controller mode or Non-Domain mode. It displays "Using the 'domainname' Windows domain" if Lotus Foundations is in Domain Member mode. It also displays the number of Lotus Foundations user licenses available for use. |
| Web Mail | When Lotus Foundations Start is installed, and once the Foundations Start add-on is installed, this displays the URL for Lotus iNotes®. |
| Virus definition updates | If the Virus Scanner is licensed and if the File Virus Scanner and/or Mail Virus Scanner are enabled, it displays when the virus definitions were last updated, how many viruses you are protected against, and links to a report on how many viruses were detected since the last reboot. |
| File virus scanner | If the Virus Scanner is licensed and File Virus Scanner is enabled, it displays: <ul style="list-style-type: none"> • How many files were scanned • How many viruses were found during the last scan once the scan has complete • How many viruses you are protected against • When the next virus definitions update will happen |
| Mail virus scanner | If the Virus Scanner is licensed and the Mail Virus Scanner enabled, it displays when the definitions were last updated and how many virulent emails have been identified since system startup. |
| Spam scanner | Displays whether or not there is a valid Spam Scanner license, and the last reported definitions update. It also displays the number of definite and probable spam that have been detected since the last reboot. |
| Printing Service | Displays the status of printing services. |
| MySQL server | Displays the status of MySQL services. The number of sessions displayed represents the number of active users currently connected to Lotus Foundations and using MySQL database services. The CPU use bar graph indicates how much processor time is being used by this service. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |

Table 1. Features of the system status screen (continued)

| | |
|---------------------|--|
| WWW server | Displays the status of Web publishing services. The number of sessions displayed represents the number of active Web sessions currently open. The CPU use bar graph indicates how much processor time is being used by this service. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |
| Secure WWW server | Displays the status of the secure Web server. The number of sessions displayed represents the number of active secure Web sessions currently open. The CPU use bar graph indicates how much processor time is being used by this service. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |
| DNS server | Displays the status of the DNS server. |
| Windows file server | Clients that are not Windows or NT can connect to this service. The number of sessions displayed represents the number of active users currently connected to Lotus Foundations and using Windows file services. The CPU use bar graph indicates how much processor time is being used by this service. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |
| Apple file server | Displays the status of file services for Apple Macintosh clients. The number of sessions displayed represents the number of users currently connected to Lotus Foundations and using Apple file services. The CPU use bar graph indicates how much processor time is being used by this service. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |
| NFS file server | Displays the status of the NFS file server for UNIX [®] and similar systems. The number of sessions displayed represents the number of active users currently connected to Lotus Foundations and using NFS file services. The CPU use bar graph indicates how much processor time is being used by this service. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |
| FTP server | Displays the status of FTP services. The number of sessions displayed represents the number of active FTP connections currently in progress. The CPU use bar graph indicates how much processor time is being used by this service. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |

Table 1. Features of the system status screen (continued)

| | |
|--------------------------------------|---|
| SMTP server | Displays the status of SMTP services. The number of sessions displayed represents the number of SMTP connections to the server. The CPU use bar graph indicates how much processor time is being used by this service. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |
| Mail queue status | Displays the number of remote email messages in the email queue. |
| IMAP Mail Server and POP Mail Server | Displays the status of servers responsible for delivery of email messages from IMAP and POP mailboxes. The number of sessions displayed represents the number of users currently downloading email messages from their IMAP or POP3 mailboxes. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. |
| LDAP Directory Server | Displays the status of the LDAP server, which is used to publish user names and email addresses into the internal directory. The number of sessions shows how many users are connected. The status is a gray box if service is disabled, a green check mark if service is operational, a yellow warning symbol if service is used heavily, and a red 'x' if there is a problem with the service. The CPU use bar graph indicates how much processor time is being used by this service. |
| Reboot button | Click this button to reboot the Lotus Foundations server. |
| Shutdown button | Click this button to properly shut-down the Lotus Foundations server. Failure to click on the Shutdown button means that your RAID array has to rebuild. See "Disk status messages" on page 112 for more information. |
| *Others | Other items might be displayed on the system status screen depending on the addition of any optional software modules. |

Notices box

In most cases, when you change a service option in WebConfig and click **Save Changes**, Lotus Foundations displays a drop-down list of major actions that are happening in the background at the top of that sub-service screen. Failure notices also are displayed in the Notices drop-down box.

System status details

The System Status Details page is a history of critical system information that has been stored by Lotus Foundations and can be viewed using an array of graphs. These graphs represent the usage of CPU load, memory usage, Ethernet traffic, and more.

Historical system status graphs

In addition to the real time status indicators on the system status page, located under these bars is a button that leads to a page which displays historical graphs of system status.

1. Click **Status** in the left side menu of WebConfig.

2. Underneath the system status is a button labeled **System Status Details**. Click this button to navigate to the historical graphs.
3. On this page is a number of graphs for various resources on the server.

These graphs incorporate a new graphical representation of server usage. The system status history graphs have been extended to include not only the average resource usage over various time periods but also the minimum and maximum resource usages experienced during these periods. The average resource usage is displayed as a brightly-colored line against a background of progressively darker colors that show the variance of resource usage over various time periods.

The most important aspect of the improved status history graphs is that it is immediately evident on all the graphs for all time periods if there is a high variance for the resource usage because the shaded backgrounds corresponding to the ranges of measurements are much wider. On the other hand, if these backgrounds are narrow, the system does not experience much variation in the resource usage at all.

Installing the Lotus Foundations Start add-on

Lotus Foundations Start introduction

Lotus Foundations Start provides the email and collaboration features using Lotus Domino. The Lotus Foundations core still provides the same features of security, backup, remote connectivity, internet uptime, and more.

Note: Lotus Foundations Start does not include bundled packages normally included in other Lotus Domino packages, such as IBM® WebSphere® Application Server, IBM WebSphere Portal Server, IBM Tivoli® Directory Integrator, or IBM DB2® Enterprise Edition packages.

Important notes: Before you start the Lotus Foundations Start installation:

- Ensure you have an administrative user account on the server named root. If the account root is not present on the system, the Lotus Foundations installation does not work properly.
- Ensure you have set up the correct host name and domain name for the server. They cannot be changed after the installation of Lotus Foundations Start. To change these, see “Changing the Lotus Foundations server host name and domain name.”

Changing the Lotus Foundations server host name and domain name

Lotus Foundations automatically assigns a random host name to the Lotus Foundations server during the first boot-up. Host names should be unique because they are used to distinguish your server from others on the local network and are used by local users to identify Lotus Foundations file and print-sharing resources. In addition, the host name, in conjunction with the domain name, forms a unique internet name under which the Lotus Foundations server and its Web, FTP, and email services are addressed on the internet.

If you want to rename your server, follow these steps:

1. Login to the Webconfig console and select **Local Network** from the menu on the left side
2. Edit the **Host Name** and **Domain Name** fields accordingly. The hostname should be unique and should contain only numbers and letters.
3. Click **Save Changes**.

After you have installed Lotus Foundations Start, the host name and domain name are no longer modifiable.

Lotus Foundations Start installation

With the Lotus Foundations Server running and configured, follow these steps:

1. If you have a DVD, insert the DVD labeled **Lotus Foundations Start Disk 2** into the server.
If you downloaded the software to a workstation, follow these steps:
 - a. Connect to the **autoinstall** file share on the Lotus Foundations Server. To do this, from a workstation, click **Start** → **Run** and then enter '\\\' followed by the server's IP address, followed by \autoinstall. For example, \\192.168.0.1\autoinstall.
Note: This does not work if Windows File Sharing is disabled. If you are using Windows Vista, you must enter the information in the text bar in the start menu. See "Setting permissions in Windows" on page 39 for more information.
 - b. Enter the administrative account and password.
 - c. Locate the folder where you unzipped the Lotus Foundations Start Lotus Domino package. The naming convention is lfstart-domino850-*nnnn*.pkg. (for example, lfstart-domino850-2760.pkg)
 - d. Drag the Domino lfstart-domino850-*nnnn*.pkg into the **autoinstall** folder. Wait for the files to be copied to the server **autoinstall** folder before you proceed.
2. At the WebConfig URL for the server, (https://domain_name:8043), select **Software Update** from the menu on the left. In the "Add-on packages available for install" section, a list of installable packages is displayed. If there is no list of available packages, wait several seconds and refresh the screen again. The Lotus Foundations Start package should be listed and displayed as: "Lotus Foundations Start 1.1 (Team autoinstall/lfstart-domino-850-*nnnn*.pkg)" or "Lotus Foundations Start 1.1 (CD-ROM)."
3. Click **Install** next to the Lotus Foundations Start add-on; read and accept the license agreements. The installation begins immediately, but the entire installation process may take up to 30 minutes.
4. Click **Status** from the menu on the left and scroll to the Add-ons section. A green check mark is displayed to the left of the product after installation that verifies Lotus Foundations Start has installed successfully. The product automatically runs. There is no need to turn it on.



Figure 7. Add-on running

Execution control list (ECL) alerts

Lotus Foundations Start is configured with a policy that has Lotus Notes® clients connect to the Lotus Domino server and refresh the users Execution control list (ECL) settings when it is installed. Permissions are determined based on the signature of the server or individual who authorized, or signed, the formula or script. In Lotus Foundations Start, the administrator of the Foundations server receives an email after installation that includes a link to the AppStart setup application that enables him or her to add the Foundations Start server and any system administrators to the authorized signature list. It is important for the administrator to set up the server ECL as any future AppStart applications that are installed are signed under the Foundations Start ID. On new Lotus Notes client installations, the first refresh happens automatically. Any future updates are received on subsequent connections to the server. The AppStart setup should be run prior to the installation of the Lotus Notes clients. By setting up the ECL, end users are not prompted for permission to execute those items that have been installed or authorized by Foundations server administrator.

Modifying the ECL list

Immediately after installing Lotus Foundations Start, the administrators on the server receive an email providing a Lotus Notes link to the Lotus Foundations AppStart administrator's page.

This page contains a link to instructions for modifying and adding administrators as trusted senders of Lotus Domino related actions. By adding these administrators, users do not have to accept these warnings, as they are authorized automatically by the Lotus Notes client.

Recognizing and accepting ECL alerts

For any existing sites that already have Lotus Notes clients installed, you might encounter the circumstance where users have to accept the security alert at least once.

If the application is signed by a known administrator on the server, select the "Start Trusting the signer..." option.

Configuring Lotus Foundations

Proceeding with configuration

You are ready to proceed with the system configuration for network settings after you have:

1. Configured your workstation to use TCP/IP.
2. Created an administrator account.
3. Logged in and connected to WebConfig.
4. Configured disks. For instructions, see "Disk management" on page 110 for details on configuring your disks.

Note: Some Lotus Foundations services are not enabled unless hard disks are configured through the WebConfig menu. For more information on configuring your disks, see "Disk management" on page 110.

Configuring General Network Settings

Follow these steps for general network configuration:

1. Select **Local Network** from the left-side menu of the WebConfig console. This displays the **Basic Setup** tab on the Local Network Setup screen.

Note that the **Host Name** and **Domain Name** fields are only editable if you have not installed Lotus Foundations Start. After Lotus Foundations Start is installed, those fields can no longer be modified.

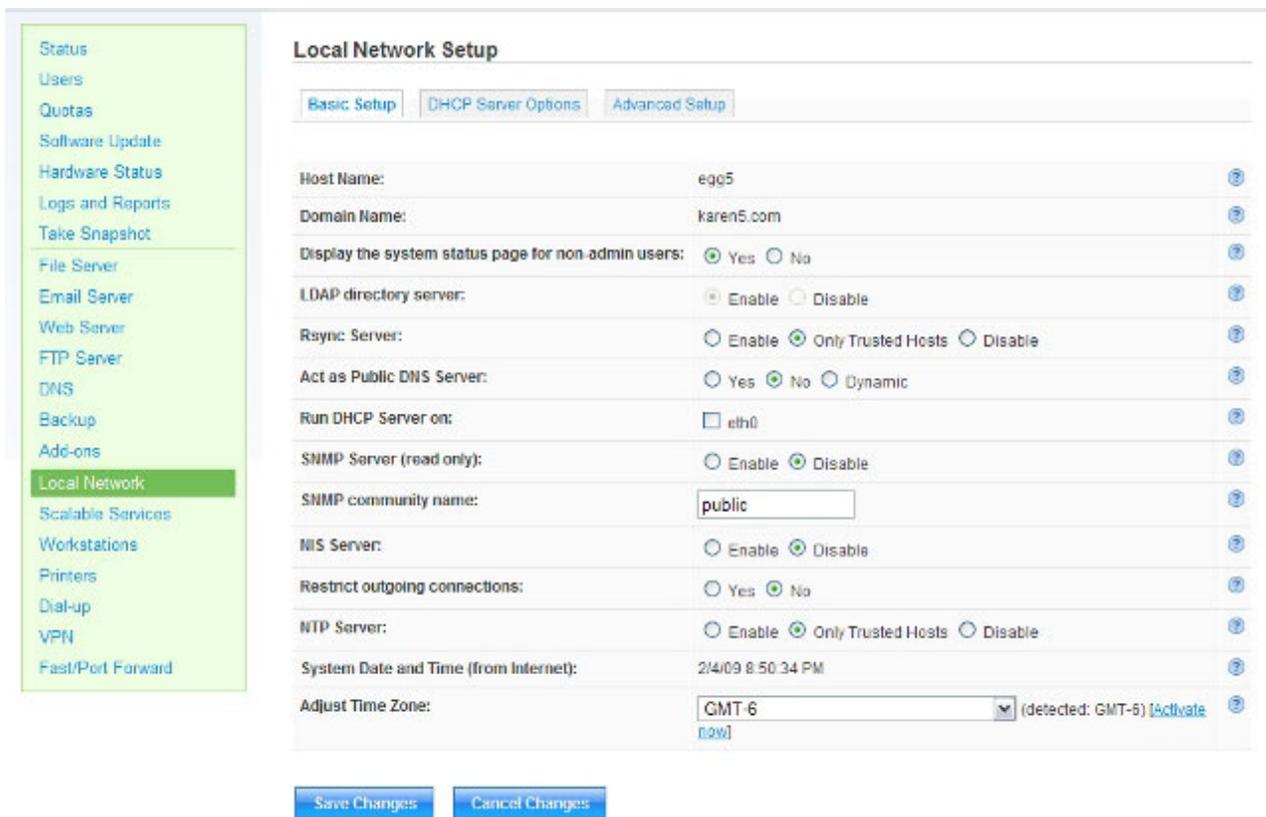


Figure 8. Local Network Setup section of the WebConfig console

2. Indicate whether or not you want to display the system status page for non-admin users on users' personal WebConfig screens.
3. Indicate whether or not you want the rsync server to be enabled. This option is for Unix-style clients only. Leave the default setting.
4. Select the appropriate public DNS resolution option:
 - Select **Yes** if you want Lotus Foundations to perform DNS resolution for Internet hosts.
 - Select **No** if you do not want Lotus Foundations to perform DNS resolution.
 - Select **Dynamic** if you want Lotus Foundations to perform Dynamic DNS resolution.

If the public DNS server is enabled, internet hosts can resolve name-to-IP number queries for internet services provided by Lotus Foundations. Dynamic DNS resolution helps you to host email, Web, and FTP services using an internet connection with a dynamic IP address.

5. The DHCP server is disabled on all network interfaces by default and presumes there is no other DHCP server on the target LAN segment. Click the checkbox beside the interface name to enable this service.
6. Indicate whether or not you want to enable the Simple Network Management Protocol (SNMP) server.
 - SNMP is used to collect statistical information from the host about parameters such as network throughput and CPU use. It is also used for network monitoring.
7. If you enable the SNMP server, enter an appropriate SNMP community name.
8. Indicate whether or not you want to enable the Network Information Server (NIS). Leave NIS disabled if you are using Windows. If you are using Unix or a similar system, leave it disabled unless you need NIS Service.

- Lotus Foundations built-in NIS is used to share user names and groups across a network to simplify user access. Unix and similar systems can be configured to use NIS. Lotus Foundations uses NIS version 2.
9. Indicate whether or not you want to enable Lotus Foundations as a Network Time Protocol (NTP) Server.
 - An NTP client is required to synchronize the desktop clocks to the Lotus Foundations server.
 10. Choose whether or not to restrict outgoing connections.
 - Lotus Foundations can restrict outgoing connections to a few protocols. Enabling this option enables outgoing traffic based on the server's configuration. All other traffic is blocked. See "Firewall services" on page 99 for more information.
 11. Lotus Foundations synchronizes its clock with a source on the Internet. To set the proper time, select your Time Zone from the drop-down list. Lotus Foundations attempts to auto-detect the proper time-zone and display its detected results for you.
 12. Click **Save Changes**.

Configuring advanced DHCP settings

To access the advanced DHCP settings, in the WebConfig console, select **Local Network** from the left-side menu. Select the **DHCP Server Options** tab.

DHCP lease length

For each interface that has DHCP enabled on it, a row is displayed listing the Interface, Length, and Actions you can perform on it. You can click the edit button on any of these rows to select the lease time that should be applied to that interface.

DHCP ranges

This is a list of ranges, giving Interface, the Range, and Actions you can perform on them. You can create a new DHCP range by clicking **New DHCP Range**.

1. Choose a starting IP address and ending IP address that you want to have the DHCP server give out.
2. Click **Save Changes** for it to take effect.

You can edit the ranges in a similar fashion by selecting the edit action button in the DHCP Ranges list.

Static DHCP leases

Static DHCP leases help you to choose which workstation receives a particular IP address by assigning that IP to its MAC Address.

1. Click **New Static DHCP**.
2. Enter the interface on which this static lease should occur.
3. Enter the MAC address of the workstation to receive an IP.
4. Enter the IP address that the workstation should receive.

You can edit leases in a similar fashion by clicking the edit button in the Action column of the Static DHCP leases list.

DHCP leases

You can see a table of current leases that have been served to workstations by clicking **DHCP Leases**. You can determine which MAC addresses are currently receiving specific IP addresses.

Configuring advanced network settings

To access the advanced network settings, in the WebConfig console, select **Local Network** from the left-side menu. Select the **Advanced Setup** tab.

The **Advanced Setup** tab helps you to configure some of Lotus Foundations more advanced features. Changing advanced network settings can potentially cause odd behavior in a network. For example, if you change a Lotus Foundations server's IP address or network mask to an incorrect value, you might not be able to reach it from your Web browser to change it back. If something goes wrong with these settings, you might be forced to change them back by logging into the local console menu or use the control panel on the front of a Lotus Foundations Appliance.

If you intend to use TunnelVision or IPsec, every network in each office location that is connected through a VPN must have a separate network subnet. If Lotus Foundations servers in various locations auto-configure their local network interfaces to the same subnet, you have to change your subnet number and IP address to a different value. Refer to "Reconfiguring network devices" on page 20 for information.

Advanced network settings screen

Follow these steps to access the advanced network settings screen:

1. Click **Local Network** in the left-side menu of WebConfig.
2. Click **Advanced Setup**. The Advanced Setup screen is displayed.

Network devices

The following list describes the network devices section of the screen:

Table 2. Network device description

| Column | Description |
|------------|--|
| Device | Lists the network interfaces installed on the Lotus Foundations server. eth0 should be connected to the LAN. eth1 and eth2 should be connected to the Internet. |
| IP Address | Lists the IP addresses to the interfaces. |
| Netmask | Lists the IP network mask assigned to a particular interface. |
| Mode | Describes how an IP address was assigned to an interface. <ul style="list-style-type: none">• "Forced" means that a permanent IP address was assigned by an administrator. eth0 should always have a forced IP address.• "DHCP" means that a temporary IP address was assigned by the DHCP server. DHCP addresses change each time you turn-on your Lotus Foundations-powered server.• "NetMap" indicates that the IP address was automatically assigned by Lotus Foundations. |

Table 2. Network device description (continued)

| | |
|---------------|--|
| Trust | <p>An important parameter that needs to be set with careful consideration.</p> <ul style="list-style-type: none"> • "Yes" signifies a trusting relationship with all hosts attached to that interface (meaning that no firewall protection is applied to that interface). eth0 is always configured as trusted. • "No" means that any traffic arriving at that interface is considered non-trusted. As such, appropriate firewall protection is applied. All Internet connections should be configured as non-trusted. |
| Action Button | <p>Click this button to display a screen where interface settings can be changed.</p> |

Reconfiguring network devices

1. Select **Local Network** from the left-side menu of WebConfig. The Local Network Options screen is displayed.
2. Click the **Advanced Setup** tab. The Network Devices list is displayed. Click an interface's Action button . The Network Settings screen for that interface is displayed.
3. *Optional:* Enter a new IP address in the format 192.168.12.10.
4. *Optional:* Enter a new network mask in the format 255.255.255.0.
5. *Optional:* Indicate whether or not to trust computers on this network.
6. *Optional:* Indicate whether or not you want Lotus Foundations to automatically choose an IP address and network mask.
 - If it is set to **Yes**, Lotus Foundations automatically selects an IP address and network mask.
 - If it is set to **No** (and autoconfiguration is disabled), you can enter an IP address or a new network mask and click **Save Changes**.
 - eth0 should never be set to choose automatically. When an IP has been chosen, the interface should have its option forced (not automatic) unless you are running a separate DHCP server on the local network.
7. *Optional:* If you have a DHCP service, for example, your internet service provider and they specify that you need to have a DHCP Client ID when setting up your network, enter it here.
8. *Optional:* Indicate whether or not you want Lotus Foundations to use this link as the default gateway.
 - If this is set to **Yes**, Lotus Foundations creates a default route to the network through this interface at the highest priority level, so this link is used by default for incoming and outgoing traffic.
 - If this is set to **Only as last resort**, Lotus Foundations creates a default route to the network through this interface with a lower priority level, so it is used only if your higher-priority (Yes) links stop working.
9. Click **Save Changes**.

Network routes

The Network routes section of the screen displays the IP routes known to Lotus Foundations. Because Lotus Foundations automatically discovers its network surroundings and sets up routing tables, you generally do not need to edit them. However, depending on your Internet connection, your ISP might assign you a new route, in which case you have to edit the default route.

Whether or not you have to change any route settings depends on your network setup and Lotus Foundations connection to the LAN and to the internet.

Deleting network routes

1. Select **Local Network** from the left-side menu of WebConfig. The Local Network Setup screen is displayed.
2. Click the **Advanced Setup** tab.
3. Click the appropriate route's delete button .
4. In the window that is displayed, confirm the deletion by clicking **OK**.

If the server prevents the route from being deleted, the server deems the route as required or important, as it must relate to another setting or subnet in the device list. If you continue to have issues, contact support. For information on Netscan, refer to the knowledge base article at the following URL:

<http://kb.nitix.com/2565>

Editing network routes

1. Select **Local Network** from the left-side menu of WebConfig. The Local Network Setup screen is displayed.
2. Click the **Advanced Setup** tab.
3. Click the appropriate route's edit action button . The Modify Route screen is displayed.
4. *Optional:* Enter a new destination IP address and netmask (in the format 192.168.12.0/24).
5. *Optional:* Click the **Interface** drop-down and select the interface over which this network can be accessed.
6. *Optional:* If this is not a local network route entry (eth1 or eth2), enter the network's gateway address.
7. Click **Save Changes**.

Network configuration scenarios

Prior to configuring the server in any of these scenarios, you must first ensure that the server has been activated with the provided activation key. If your configuration scenario supports internet connectivity, you can activate at anytime. Remember, Lotus Foundations expires in 30 days without activation.

1. **Scenario:** Lotus Foundations server as a workgroup server without a direct connection to the Internet

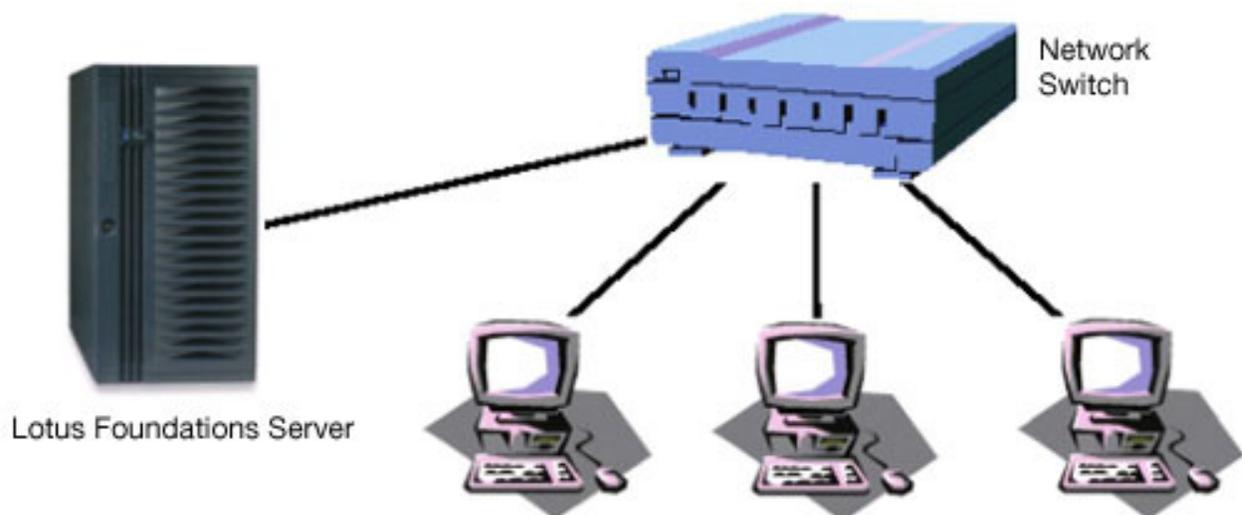


Figure 9. Diagram of scenario 1

In this scenario, you would go to the Advanced Setup screen to change the IP address or the network mask of the local network interface or Lotus Foundations default route. Although you generally do not need to change these settings, you can still do so:

- a. Select **Local Network** from the left-side menu of WebConfig.
 - b. Click **Advanced Setup**. The Advanced Setup screen is displayed.
 - c. In the Network Devices or Network Routes section of the Advanced Setup screen, click the appropriate action button.
 - d. Depending on your choice, the Modify Route or the Network Settings screen is displayed. Refer to "Reconfiguring network devices" on page 20 and "Editing network routes" on page 21 for full descriptions of these two screens.
 - e. Change the appropriate settings and click **Save Changes**.
2. **Scenario:** Lotus Foundations server as a workgroup server and dial-up gateway to the Internet



Figure 10. Diagram of scenario 2

If Lotus Foundations has automatically chosen the proper IP addresses, there is nothing else for you to change. If you want to change the Lotus Foundations-powered server's local IP addresses, you can do so by clicking the edit button on the line describing the parameters for the Ethernet 0 interface.

The default route is automatically determined when Lotus Foundations dials in to the Internet. In this case, there should be no default route entry in the Routes Table.

3. **Scenario:** Lotus Foundations server as a workgroup server and high-speed gateway to the Internet

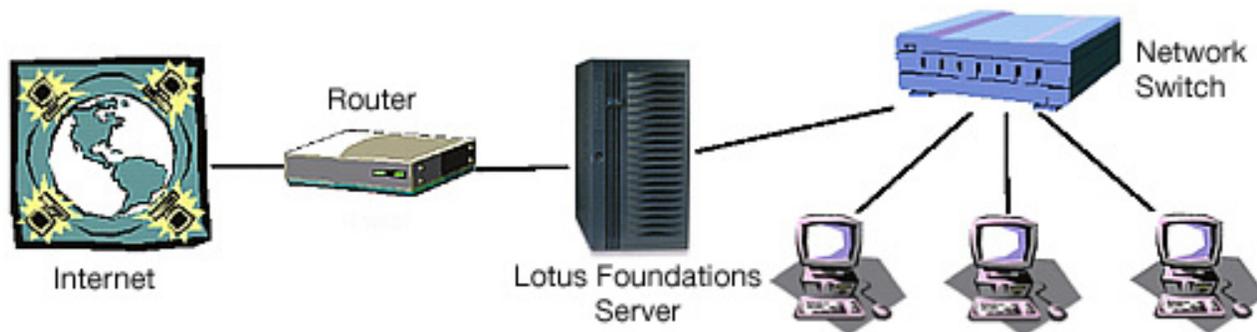


Figure 11. Diagram of scenario 3

Lotus Foundations auto-configures its parameters if the ISP uses DHCP as a means of automatic network configuration. In this case, there should be nothing for you to do on the Advanced Setup screen, although you can change the address of your local network interface if you want to do so.

If the ISP assigns a unique static IP address, network mask, and default route, Lotus Foundations discovers the proper default route, but does not know which IP address to select. Although Lotus Foundations finds the available address and establishes a proper connection to the internet, you

should change the IP address of the Internet interface to the address assigned by your ISP. You should do the same with the default route setting. If you run into problems configuring advanced network settings, contact technical support. If you run into problems configuring advanced network settings, refer to the list of knowledgebase articles at the following URL:

<http://kb.nitix.com/1426>

To change these settings:

- a. In the Network Devices section of the Advanced Setup screen, click the appropriate port's (for example, eth1) action button.
 - b. The Network Settings screen is displayed. Enter the new IP address and click **Save Changes**.
 - c. In the Network Routes section of the Advanced Setup screen, click the action button  in the **Default** row, which is the last entry in the list.
 - d. The Modify Route screen is displayed. Change the default route and click **Save Changes**.
4. **Scenario:** Lotus Foundations server as a domain controller and high-speed gateway to the Internet.

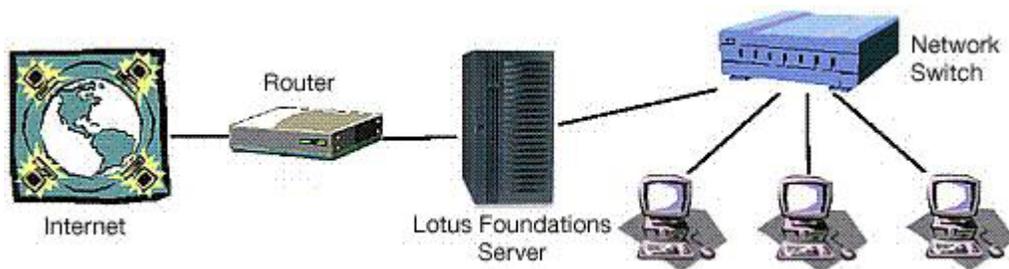


Figure 12. Diagram of scenario 4

Lotus Foundations can serve as a Windows NT[®] style domain controller for all the computers running Windows on the network. As the domain controller, Lotus Foundations provides authentication services for the computers on the network. When this function is enabled, the Windows file server is set up as a domain controller, and a domain replaces the Windows workgroup. For specific information about configuring domain controllers, see "NT domain services" on page 41.

Configuring your internet connection

Configuring a cable modem

No extra tasks are required for configuring a cable modem.

Configuring a DSL connection

1. Select **Dial-up** from the left-side menu of WebConfig. The Dial-up Networking Setup screen is displayed.
2. Click the action button in the appropriate ADSL row (eth1 or eth2 only). The ADSL Dialer Options screen is displayed.
3. Enter the Internet account username provided by the ISP.
4. Enter the account password provided by the ISP.
5. Re-enter your password to ensure it was entered correctly. If the passwords do not match, you are asked to re-enter your password in both fields.
6. *Optional:* Enter your gateway IP address. Leave this blank if you do not know the address.
7. Indicate whether or not you want to enable the connection.
 - Select **Yes** if you want to establish a permanent connection.
 - Select **No** if you do not want to establish a connection.

- Select **Only as a last resort** if you want to use this connection only if the primary connection fails.
8. Click **Save Changes**.

Configuring a dial-up modem

The Lotus Foundations Appliance does not come with pre-installed modems. The following instructions are for configuring services if you have a device attached which is auto-detected by the Lotus Foundations server. Refer to your hardware vendor for details on installing third-party components.

1. Select **Dial-up** from the left-side menu of WebConfig. The Dial-up Networking Setup screen is displayed.
2. *Optional:* If you have an external modem connected, you might need to click Detect Modems to initiate the Modem Detection Cycle. Refer to “DoubleVision” on page 26 for information on using multiple dial-up modems.
 - If the modem is undetected, check cables and power. Cycle power on the modem and initiate a new Detect Modems test.
3. Click the Modem #1 action button. The Dial-up networking setup screen is displayed.
4. Enter the phone number provided by your ISP. If you have to dial 9 to get an outside line, enter this number. For example, enter: 9, 123-123-1234.
5. Enter the Internet account username provided by your ISP.
6. Enter the account password provided by your ISP.
7. Re-enter your password to ensure that it was entered correctly. If the passwords do not match, you are asked to re-enter your password in both fields.
8. Indicate the number of idle seconds before automatic disconnection.
 - If you enter zero, the connection never automatically disconnects. Be careful with this setting, especially if you do not have an unlimited internet access package from your ISP.
9. Select the appropriate dialing mode:
 - Select **Yes** if you want the Lotus Foundations server to dial automatically to the internet when someone tries to reach it.
 - Select **No** if you want to manually initiate a connection by clicking Dial Modem on the System Status page.
 - Select **Only as a last resort** if you want to use a dial-up connection when one or more of your high-speed connections fail. The dial-up connection stays active until one of the high-speed connections becomes functional. Although all traffic is forwarded to the high-speed connection when it returns to normal, the dial-up connection remains active for a few minutes in case the high-speed connection fails again. In that case, the system re-routes traffic back to the dial-up connection immediately without having to wait for a dial-up connection to be re-established.
10. Indicate whether or not you want your Lotus Foundations server to emulate Windows Dial-up Networking.
 - Some internet providers are setup to work only with Windows dial-up clients. If you have problems establishing dial-up connection, try enabling this option.
11. Indicate whether or not users are able to establish a remote dial-in modem connection to the internal network.
 - VPN (PPTP) and Dial-In access has to be enabled before you establish a remote connection. See “User & Team management” on page 29 for more information.
12. Click **Save Changes**.

Take a snapshot

Now that you have taken the time to configure Lotus Foundations you can use the **Take Snapshot** selection in the menu to display all the information available on one scrollable page. You can also save

this information in an offline Web Page format as reference material to cross check any changes that might occur in your configuration settings.

User licenses

User licenses help individuals within a company to legally use the Lotus Foundations platform. When you purchase a Lotus Foundations user license, you are purchasing the rights for a user to use the software.

User licensing requirements

Lotus Foundations uses a "Per User" and a "Per Server" licensing model. Any number of individuals can connect to the Lotus Foundations server; however, you must purchase a Lotus Foundations User License for each individual, or "user account," where access to Lotus Foundations services, such as email, file, print, MySQL and FTP services is needed. A server license is required for every Lotus Foundations Server deployed.

Lotus Foundations user licenses are not required for team accounts without a password. Team members can still access team data/services using their personal user account passwords. If you choose to assign a password to a team, this counts towards your total user license usage.

A user license is required for every user who accesses Lotus Foundations Start, however one additional "free" Lotus Foundations user license is allocated for a Lotus Foundations administrator.

Note: The following Lotus Foundations product features are not enabled for the trial license:

- Anti-virus
- Anti-spam
- Engate

License information

To see how many Lotus Foundations users are licensed for the system and how many licenses are currently being used, follow these steps:

1. Log in to WebConfig with your administrator username and password.
2. Select **Software Update** from the WebConfig screen.
3. Click the **Licenses** tab.
4. The Software Update screen is displayed with a Notices box at the top of the screen showing how many Lotus Foundations users you have.

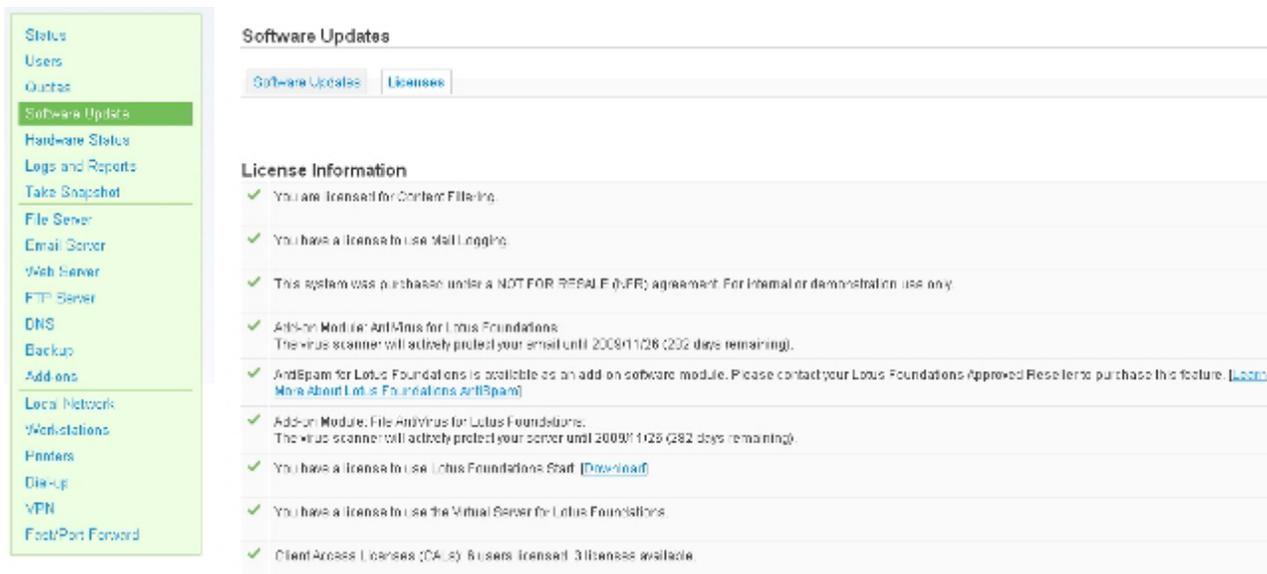


Figure 13. Licenses screen in the WebConfig console

Additionally, the **User Authentication Method** line on WebConfig’s main System Status screen displays how many Lotus Foundations users have licenses for the system and how many are currently being used.

If you exceed your licensed number of Lotus Foundations Start users, a Notices box is displayed at the top of each page in the WebConfig console. To purchase additional Lotus Foundations Start licenses, contact your authorized reselling partner.

DoubleVision

What is DoubleVision?

DoubleVision is a Lotus Foundations feature that helps you to configure two or more internet connections. For example, you can combine a cable modem and an ADSL link, two ADSL links, multiple dial-up modems to the same ISP or different ISPs, or any combination of internet connections supported by Lotus Foundations.

There is no single place to configure DoubleVision. Instead, it is automatically configured when more than one internet connection is used at the same time.

Note: For DoubleVision to activate, you must have at least two gateway connections. You can choose a default connection.

What DoubleVision offers

Using DoubleVision technology, Lotus Foundations helps you to set up multiple internet connections and use them all simultaneously. DoubleVision does not bond your internet connections into a single pipe. It manages the connections independently.

- You can have two ADSL lines and subscribe to two different ADSL services, so if either service fails, you are still online. When both services are working, your connection is twice as fast.
- You can have a cable modem and an ADSL line at the same time and share the load between them.
- In areas without high-speed internet support, you can configure multiple dial-up modems using multiple accounts, and reach ISDN-equivalent speeds at a fraction of the price.

- You can set up a dial-up modem as a fallback connection. Lotus Foundations automatically switches to your dial-up ISP when your normal internet connection (one or more ADSL, cable, or other high-speed lines) fails.

Table 3. Advantages to DoubleVision

| Advantage | Description |
|--------------------------|--|
| Increased performance | Internet traffic is increased by being able to use the bandwidth of both lines. You cannot specify which connection is used. It is automatically chosen by Lotus Foundations. |
| Increased reliability | If one ISP's internet connections fails, the remaining ISP's connection stays functional. This means that your downtime is limited, also known as fail-over, or redundant connectivity. |
| Last Resort dial-up mode | If one or more of your high-speed internet connections fail, Lotus Foundations can dial your modem automatically and use dial-up access instead. When your high-speed links are restored, the modem automatically disconnects after it verifies that the high-speed connections are stable and active. The same applies to high-speed connections if you choose to use them as a last resort connection. |
| Dynamic DNS Integration | If you are using Dynamic DNS, Lotus Foundations automatically publishes appropriate DNS names so people can always find your Web site, even if your high speed links are down and you need to use a dial-up connection. See "Domain Name Service" on page 101 for more information. |
| Full automation | You do not have to reconfigure any client workstations on your local network to take advantage of DoubleVision. DoubleVision is fully automated and managed by the server. No human intervention is required to activate and deactivate internet services when they fail or are restored. Lotus Foundations automatically takes care of these situations. |

Modem connections

Since modems are normally much slower than other internet connections, you probably do not want to use a modem as your primary connection. Instead, you can configure your modem as a "last resort" option, meaning that your modem only connects if one or more of the high-speed connections fails.

If a modem is configured as the primary connection, it connects to the internet even if high-speed connections are available. This is useful if you want to test the modem connection.

How internet failover and DoubleVision work

What internet failover does

- You can set up multiple links in order of priority by setting some to **Enable: As last resort** instead of **Enable: yes**. These links only get activated when the primary links are marked broken by Lotus Foundations.
- Broken links are detected using a method called Demi-Ping. It detects most kinds of link failures to the Internet, although certain kinds of partial failures cannot be detected. Lotus Foundations should always notice if you unplug the physical connection to a link and automatically switch to your secondary links, and this is the easiest way to check that it is working.

- You can see that you are using internet failover by checking the "number.letter." code next to your various Internet links on the status page of WebConfig. Ignoring the letter, the different numbers imply the different backup priorities. For example, if you have "1.a. Indirect on eth1", "1.b. Indirect on eth2", and "2.a. Modem", then your primary links (1.x) are the first two and your secondary link (2.x) is the last (modem) link.
- The DNS server, including Dynamic DNS, publishes one of the IP addresses for the "most important non-broken link" as the IP address for your domain. That is, if a #1 link is non-broken, then it publishes its address; if all #1 links are broken, then it publishes a #2 address.
- Because incoming connections are usually addressed to your domain name, whichever IP your DNS is publishing is the one to receive most incoming traffic. However, if there is more than one non-broken link, any of those should be able to receive incoming traffic if you ping the IP address of that link.
- All outgoing connections go through the first non-broken link. There is no way to force an outgoing connection to use another link.

What DoubleVision Does

- DoubleVision handles outgoing load sharing between multiple links at the same priority level. In the previous example, if you have 1.a. Indirect on eth1, 1.b. Indirect on eth2, and 2.a. Modem, then if all links are non-broken, DoubleVision divides the outgoing Web traffic between the two 1.x. links. It does not necessarily divide the traffic evenly.
- DoubleVision's load sharing works differently from typical load balancing routers. It takes each individual session, such as a single Web page, and assigns it to one internet link or another, and all packets for that session go through the same link. This is unlike the usual load balancing routers, which split packets randomly across links, even packets belonging to the same session. This means two things:
 1. You do not need both links to be through the same co-operating ISP that can decode a single session from multiple links which is the major advantage of DoubleVision.
 2. If you only have one session at a time or your sessions are unluckily assigned to links, you get little to no performance improvement.
- Some types of outgoing traffic either cannot be or should not be load shared in this way, for example, FTP, ping, traceroute, and SMTP. This is usually because many protocols, such as FTP, ping, and traceroute use multiple TCP sessions for one logical session. SMTP is special because of spam relay protection, which makes it so you have to use a different outgoing SMTP server depending which link is in use. To avoid these problems, only use DoubleVision for outgoing Web sessions; for other kinds of sessions, Lotus Foundations chooses the best link as a "default" link and uses that for all outgoing non-HTTP traffic. In practice this is not much of a problem, because almost all high-bandwidth traffic comes from the Web.
- Incoming traffic is treated differently from outgoing traffic: Lotus Foundations accepts connections on all non-broken links, but the DNS for your domain name is only registered to point at the default link chosen by Lotus Foundations. This is because you cannot actually tell client software to use the best link or alternate between these two links in a reasonable way, so Lotus Foundations has to choose the best one and tell them to use that. Occasionally, the DNS-advertised best link starts to get too loaded down, probably because all the incoming traffic is using it, so Lotus Foundations decides to advertise the second-best link for a while instead. Of course, remote users may have a DNS cache of 5 minutes or more, so this change does not take effect immediately.

DoubleVision quick summary

- You are using internet failover if you have multiple links with different numbers: "1.a.", "2.a.", etc.
- You are using Double Vision if you have more than one highest-priority non-broken link with the same number and more than one letter: "2.a.", "2.b.", etc.
- With either Double Vision or internet failover, unplugging any link should cause Lotus Foundations to switch you over to a different, working one. If it does not, something is misconfigured or you have encountered one of the following limitations.

- Your DNS server always publishes the address of its favorite non-broken, high-priority link. So incoming traffic generally comes in on that address.
- Incoming traffic is always accepted at the address of any non-broken link, even if DNS currently gives users no way of actually getting there.
- Outgoing Web traffic always goes through all highest-priority DoubleVision links.
- Outgoing non-Web traffic always goes through Lotus Foundations' favorite highest-priority link.

User & Team management

Service integration

User and team management is integrated with a number of other Lotus Foundations services. It is important that you understand how user and team management relates to these other functions before creating, editing, and deleting users and teams. Read the following section carefully.

Lotus Foundations email, file, Web, and FTP services are tightly integrated. Every user and team account that is created has instant and automatic access to all of these services. When a user is created, a number of things happen in the background:

- A login account is created and the password defined by the administrator is assigned to that account.
- A personal User directory is created on the server. This directory is accessible in Windows' Network Neighborhood or on Macintosh's AppleShare drive. If NFS is enabled, UNIX and similar systems can use the path `/export/home/USERNAME` to access this directory. For example, the path for someone with the username `janedoe` would be `/export/home/janedoe`.
- A WWW directory is created within the user's personal directory. Any file stored in this directory is automatically published on the user's personal web page. This is only valid if you have the option for 'Users Personal Home Page:' set to **Enabled** or **Only Trusted Hosts**.
See Web Server in WebConfig for additional information.
- An FTP account (which points directly to the user's personal directory) is created for the user. If the user logs in to the FTP server using the proper username and password, they can access the files in their personal directory.
- An email account is created for the user. Email is available through either POP3, IMAP, or the Domino email protocol.

Similarly, when a team is created, a number of things happen in the background:

- A team login account is created and the password defined by the administrator is assigned to that account.

The default configuration is to have no password. Remember, assigning a password to a team takes up one user license.

- A Team directory is created. This directory is accessible to all Team members in Windows' Network Neighborhood or on Macintosh's AppleShare drive. If NFS is enabled, UNIX and similar systems can use the path `/export/home/TEAMNAME` to access this directory. For example, the path for a Team named `sales` would be `/export/home/sales`.
- A WWW directory is created within the team directory. Any file stored in this directory is automatically published on the team's web page.
- An FTP account (which points directly to the team directory) is created for the team. If a team member logs into the FTP server using the proper team name and password, they can access the files in the team directory.
- An email distribution account is created for members of the team. Team email can be accessed through either POP3 or IMAP mailboxes. Email received by the Team email account can be set to be automatically forwarded to all members of the Team.

Note: All Lotus Foundations user and team accounts with a password require a Lotus Foundations user license. Lotus Foundations user licenses are not required for team accounts without a password; team members can still access team data/services using their personal User account passwords. Users who do not need to access Lotus Foundations services (such as email, file, print, MySQL, and FTP services), do not require a user license. One additional "free" Lotus Foundations user license is allocated for a Lotus Foundations administrator. See "User licenses" on page 25 for more information.

User accounts

Browsing users

Users are listed in the Users section of the WebConfig console. You can search for users and teams by user ID, Team ID or full name.

Disabled users are displayed in this list with '(disabled)' appended to the **Full Name** field. Users are considered disabled when they have no password set.

Creating users

Follow these steps to create users:

1. Select **Users** from the left-side menu of WebConfig.
2. Click the **Users** tab.
3. Click **Add User**.

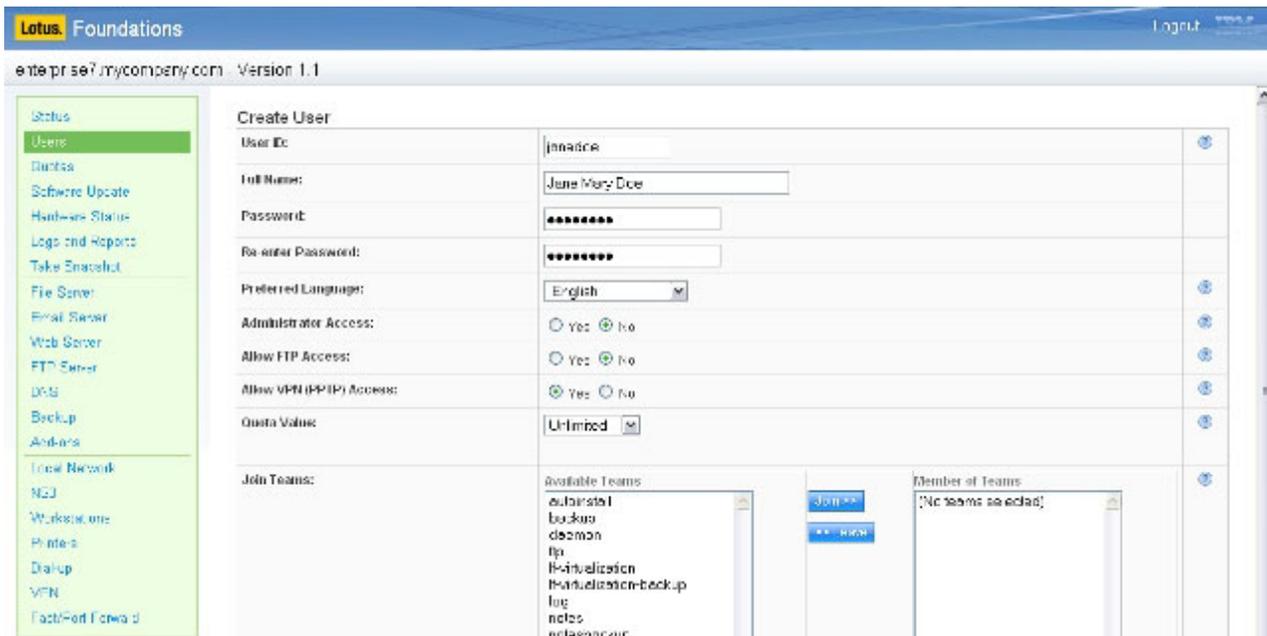


Figure 14. Creating a user in the WebConfig console

4. Enter the User ID (also known as a "username") that serves as the User's login and personal directory name.

Note: User IDs cannot contain spaces or any punctuation other than hyphens, periods, and underscores, for example, jane-doe, jane.doe, jane_doe are all acceptable user IDs.

- With Lotus Foundations Start installed, this user ID becomes part of the user's email address. For example, if the username janedoe is created on a Lotus Foundations server that resides in the example.com domain, Jane's email address is janedoe@example.com.

5. Enter the user's full name. This full name must be unique to all other names when running Lotus Foundations Start.
6. Enter a password for the user. User passwords should also be unique to help maximize security and access controls.
7. Re-enter the password to ensure that it has been entered correctly. If the passwords do not match, you are asked to re-enter the password in both fields.
8. Select a preferred language for the user. This determines the language for the email template and for the Lotus Notes client through the one-click installation.
9. Indicate whether or not this user has administrative privileges.
 - Administration privileges means that this user has unrestricted access to all configuration functions of Lotus Foundations. If you give a user administrative privileges, disk and email quota values are not configurable. Administrative users automatically have unlimited quotas.
10. Indicate whether or not this user has FTP access to his or her private directory.
 - The FTP file server has to be enabled before the user can have FTP access. If FTP is enabled in Trusted Hosts Only mode, the user can access files from a trusted, internal network or from a VPN. If FTP is enabled in open mode, the user can access files using FTP from anywhere on the Internet.
11. Indicate whether or not the user is allowed to establish a remote VPN (PPTP) or dial-in modem connection to the internal network.
 - For security reasons, most users should not be able to establish a remote connection. VPN services must be enabled before a user can establish a VPN connection. Similarly, dial-in for a specific modem has to be enabled before a user can establish a dial-in connection on that modem. See "Remote access services" on page 95 for more information.
12. If the domain controller is enabled, choose a drive that the user's files can be automatically mounted to when logged into a domain workstation. The default drive is X:.
 - Be sure to choose a drive that is not already in use. For more information, see "NT domain services" on page 41.
13. Select a quota value for this user. For more information, see "Disk quotas" on page 40.
14. Select an email quota value for this user. This is the total amount of disk space a user's email file can occupy.
15. Enter any nicknames that are required for this user. Email sent to any of these nicknames are delivered to this user.
16. Under **Join Teams**, select the team(s) from the **Available Teams** list that this user is a part of. Click **Join**. The teams are displayed in the **Member of Teams** box.

Note: Team membership gives users full access to the team's shared directory. If one of the joined teams is a member of any other team(s), when it is added to the Member of Teams list it has (# inherited) listed after it. The user has "inherited" team membership to those other team(s).
17. Click **Save Changes**. This returns you to the main User Setup page, and the user is displayed in the list of previously created users.

Editing users

Follow these step to edit users:

1. On the User Setup page, click the **Users** tab. Click the appropriate user's edit icon . The Modify User screen is displayed.

Note: While running Lotus Foundations Start, user and team names are not modifiable.

2. Change the user's information as necessary. Refer to "Creating users" on page 30 for a description of the fields on this screen.

3. Click **Save Changes**.

Other Actions

- Remove a user's password to disable the account.
- Enter a password for a disabled user to re-enable him or her.

Deleting Users

Note: Deleting a user means that all of the user's personal files, email settings, mailbox, and any undelivered email in the mailbox is deleted. Once this is done, none of the above can be recovered (unless you restore the data from a previous backup).

To delete an individual user:

1. On the User Setup page, click the **Users** tab. Click the appropriate user's delete icon  .
2. An "Are you sure you want to delete user" confirmation box is displayed. Click **OK** to continue and delete the user.

To delete multiple users

To delete multiple users, you can use pre-existing pwdump2 or spreadsheet data using the following syntax:

```
username1, username2, username3, username4.
```

User names should be separated by new lines or commas.

Fields other than the username field are optional and should use the following syntax:

```
username[,user2,user3(...)]:password:full_name
```

The ":" (colon) separator can be replaced by ";" (semi-colon) or [TAB].

1. In WebConfig, click **Users** in the menu.
2. Click the **Users** tab. Click **Import Users**. The Import Users screen is displayed.
3. In the *Action* field, select **Delete Users**.
4. Right-click the field called **Import Users Info**. Select **Copy**. This copies the contents of the file.
5. Click **Save Changes**.

Import users from Windows

Follow these steps to upload user information from a Windows 2000 or NT server:

1. You need to download an executable file called pwdump2. The program is freely available online and can be found at various locations on the Internet.
2. Download the file called pwdump2.zip and unzip the contents to its own folder. For example, extract the contents to a folder called pwdump2 on your C drive.
3. Click **Start**, and select **Run**.
4. Enter cmd, then click **OK**.
5. Type the following, then press Enter:
cd pwdump2
6. This changes the directory to the folder you created on your C drive that contains the contents to the file pwdump2.zip.
7. Type the following, then press Enter:
pwdump2 > list.txt

8. This runs the file called `pwdump2.exe` and generates a text file called `list.txt` in the same folder.
9. Open the file called `list.txt`. This contains a list of Windows users. Highlight the users that you wish to import, right-click and choose **Copy**.
10. In WebConfig, click **Users** in the menu. Click the **Users** tab.
11. Click **Import Users**.
12. Right-click the field labeled Import Users Info. Select Paste. This copies the contents of the file called `list.txt` into this space.
13. When importing users, you can specify each user's quota value as small, medium, or large by using the following syntax:
`username[,user2,user3(...)]:password:full_name:quota.`
14. Click **Save Changes**. The Import Users screen is displayed.
15. Click **Save Changes**.

For more information on quota values, see "Disk quotas" on page 40.

Because Windows uses a one-way hash algorithm for storage of passwords, the passwords are not easily recovered. The administrator needs to create new passwords for each imported user from the Modify User screen.

You can only import either a block of `pwdump2`-generated data or a block of spreadsheet-generated data at one time. If you need to import both, import each type separately.

Modifying user email settings

1. Click **Users** from the left-side menu of WebConfig. Click the **Users** tab. The main User Setup screen is displayed.
2. Click the appropriate user's edit action button. The Modify User screen is displayed.
3. Click **User Email Settings** located at the bottom of the screen.

The following fields are displayed on the user email page:

- **Retrieve Mail from POP Server:**
 - Used to pull POP mail from one account from a mail provider or a third party POP mail provider, for example, Yahoo/Hotmail.
 - Configure by entering the full server name used to pull mail down from your ISP, for example, `pop1.isp_server.com`.
- **Remote POP Username:**
 - Enter the appropriate account credentials for the mail service you are retrieving from.
- **Remote POP Password:**
 - Enter the password for the POP account.
- **Re-enter POP Password:**
 - Re-enter the password for the POP account to ensure that it was typed correctly.

For more information about the following Spam related fields, see "Spam scanner" on page 142.

Team accounts

Creating teams

Follow these steps to create teams:

1. Select **Users** from left-side menu of WebConfig. Click the **Teams** tab. The main User Setup screen is displayed.

2. Click **Add Team**. The Create New Team screen is displayed.

| Create Team | |
|--------------------------|--|
| Team ID: | <input type="text" value="testteam"/> |
| Full Name: | <input type="text" value="Test Team"/> |
| Password: | <input type="password" value="....."/> |
| Re-enter Password: | <input type="password" value="....."/> |
| Preferred Language: | <input type="text" value="English"/> |
| Allow FTP Access: | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Allow VPN (PPTP) Access: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| Create team as: | <input checked="" type="radio"/> Normal Team <input type="radio"/> Room <input type="radio"/> Resource |
| Room Capacity: | <input type="text" value="10"/> |
| Quota Value: | <input type="text" value="Unlimited"/> |

Figure 15. Creating a team in the WebConfig console

3. Enter a team ID.
 - This ID serves as the name of the team’s shared directory and as the team’s FTP login name, which gives team members FTP access to the shared directory and the WWW directory. Team IDs cannot contain spaces or any punctuation other than hyphens, periods, or underscores.
4. Enter a descriptive name for the team in the Full Name field. This descriptive name must be unique.
5. Enter a login password for the team. Team passwords should be unique.
6. Re-enter the password to ensure it was entered correctly. If the passwords do not match, you are asked to re-enter the password in both fields.
7. Select a preferred language.
8. Indicate whether or not the team has FTP access to the team directory.
 - The FTP file service has to be enabled before the team can have FTP access. If FTP is enabled in Trusted Hosts Only mode, the team can access files from the internal network or from a VPN. If FTP is enabled in open mode, the team can access files using FTP from anywhere on the Internet.
9. Indicate whether or not team members are allowed to establish a remote VPN (PPTP) or dial-in modem connection to the internal network. For security reasons, most teams should not be able to establish a remote connection.
 - VPN services and dial-in services have to be enabled before a team member can establish a VPN or dial-in connection. See “Remote access services” on page 95 for more information.
10. Select the team type to create this team as:
 - Normal Team
 - Room
 - Resource

Teams created as a room or a resource can be reserved by users using Lotus Notes.
11. If you chose to create the team as a room, select the capacity of the room referred to.
12. Select a quota value for this team. For more information, see “Disk quotas” on page 40.
13. Enter any nicknames required by this team. Emails sent to any of these nicknames are delivered to the team.

14. Under Team Members, select the user(s) from the **Users** list who are a part of this team. Click **Add**. The user(s) is displayed in the **Team Members** box.
 - Team membership gives users full access to the team’s shared directory.
 - If one of the members is a team, when it is added to the **Team Members** list it has (# members) listed after it. That team’s members have inherited team membership.
15. Click **Save Changes**. This returns you to the main User Setup page, and the team is displayed in the list of previously created teams.

Editing Teams

Follow these steps to edit teams:

1. On the User Setup screen, click the **Teams** tab. Click the appropriate team’s edit icon  .
2. The Modify Team screen is displayed.

Note: While running Lotus Foundations Start, the team name and the team type are not modifiable. If you created a team as a room you cannot convert it to a resource, but you can modify the capacity of the room. Similarly if you created a team as a normal team or a resource, you cannot convert it to another team type.

3. Change team information as necessary. Refer to “Creating teams” on page 33 for a description of the fields on this screen.
4. Click **Save Changes**.

Testing email

When modifying a team, click **Send** on the **Test Email** row to send a test email to the team.

Deleting teams

Note: Deleting a team means that the team’s shared network directory and all of the files contained within the directory are deleted. Once this is done, none of the above can be recovered unless you restore the data from a previous backup.

Follow these steps to delete teams:

1. On the main User Setup screen, click the **Teams** tab. Click the appropriate team’s delete icon  .
2. In the confirmation dialog that displays, click **OK**.

Searching for teams

The User Setup screen restricts the number of entries that are displayed by default. If there are a large number of teams, only the first 10 teams are displayed in the User Setup section. At the bottom of the section there are links to a series of teams. For example, if you have 43 teams, the screen displays: [show all] [a - o] [p - y]. Clicking on the [p - y] link displays all teams with team names beginning P through Y. To help administrators to easily locate teams’ records, there is a Team Search field at the top of the User Setup screen. To search for a team, type in that team’s ID (or portion thereof) and click **Search**.

Password policy

The password policy feature helps an administrator to set restrictions on the format of passwords chosen by users. For example, the administrator can specify that uppercase and lowercase letters must be included in the password and/or that passwords must be of a particular minimum length.

Creating a password policy

Follow these steps to create a password policy:

1. Select **Users** from the left-side menu of WebConfig.
2. Click the **Password Policy** tab.
3. Choose whether or not to enforce the password policy on passwords set by administrators.
 - The password policy settings are always enforced for passwords chosen by users. If this option is enabled, the password policy settings are also enforced for passwords chosen by administrators, including their own passwords.
4. Select which password policy criteria should be enforced by checking the appropriate boxes.
 - The "Passwords must contain letters" and "Passwords must contain both uppercase and lowercase letters" rules are tied to each other. Therefore, enabling the latter settings automatically enables the former.
5. If you want to enforce a minimum password length, enter the number of characters in the Password minimum length text box. Use 0 for no minimum.
6. Click **Save Changes**.

Illegal passwords

When a password that does not conform to the policy as specified by the administrator is entered for a user, that user receives an email notifying them that they need to change their password to one that conforms to the policy. The email also includes instructions on how to perform this password change.

If a user changes their password in their personal WebConfig to one that does not meet the policy criteria, they get a pop-up error message.

An error message is also displayed in WebConfig's Notices box telling them that their password was not changed.

If the "Enforce password policy on passwords set by admins" option is set to No, Administrators are able to change a user's password to one that does not meet the policy criteria. This helps administrators to set an easy-to-remember temporary password for a new user, until that user can set his or her own password.

The administrator receives a warning message in WebConfig's Notices box informing him or her that the password does not meet the policy criteria, but that the password has been changed.

If a user is already set up and the administrator creates or changes a password policy, that user's password is valid - even if it does not meet the policy criteria - until the next time he or she logs onto WebConfig.

File services

File sharing services

Lotus Foundations is designed to provide high performance file sharing services for Windows, Macintosh, and UNIX-style clients. Files created by Windows users can transparently be seen by Macintosh users and vice versa.

The management and administration of file services is tightly integrated with user management and administration. Refer to "Service integration" on page 29 for a detailed explanation of how file sharing services are automatically set up during user and team creation.

Configuring file services

Follow these steps to configure file services:

1. Click **File Server** from the left-side menu of WebConfig. The **Basic Setup** tab is the default view.

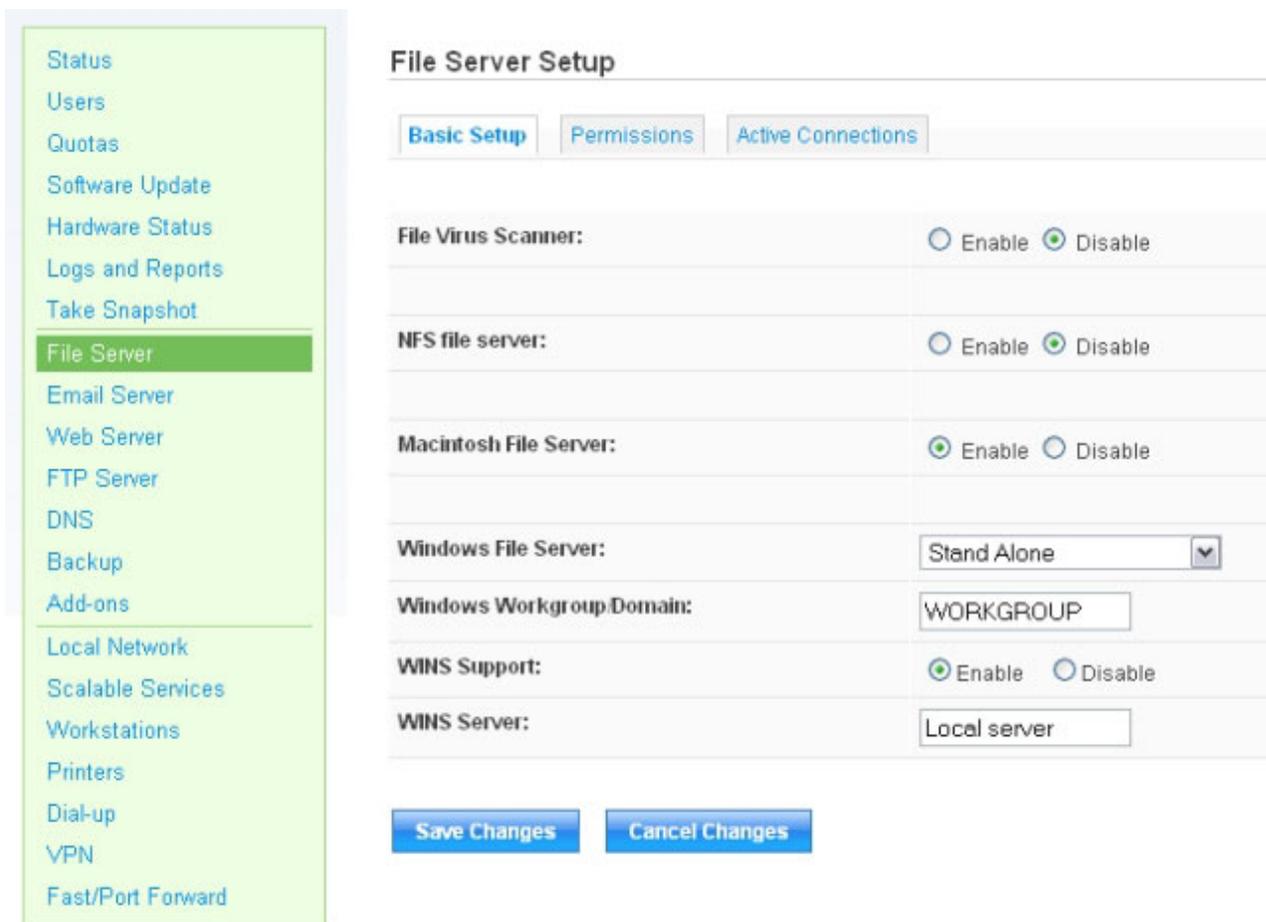


Figure 16. File Server Setup screen in the WebConfig console

2. If appropriate, enable the file virus scanner. With this option selected, all files on the system are automatically scanned for viruses every 12 hours. When a virus is encountered, it is cleaned, if possible. Otherwise, it is renamed to 'filename-INFECTED' and the user whose directory the file was found in is informed through email of the virus.
3. If appropriate, enable the NFS files server, which enables UNIX, Linux®, and similar computers to access shared directories on the server.
4. If appropriate, disable the Macintosh file server. This option enables the Appletalk Macintosh file server, which allows Macs to access shared directories on the server. Each user and team has a shared directory, accessible by Windows file sharing, FTP, Appletalk, or NFS. If you have no Macs on your network, you can safely disable this.
5. In the Windows File Server section, you can select the following from the drop-down:
 - **Stand Alone** enables the file server and is the default setting.
 - **Disabled** turns off the file server.
 - **NT Domain Controller, NT Domain Member, Active Directory Member** should be selected if the server is an NT domain controller, member or Active Directory member. Refer to "NT domain services" on page 41 for further instructions.

6. Enter a workgroup name if you are not acting as a domain member or a domain controller. This name indicates the workgroup under which the Lotus Foundations-powered server is listed as a resource in Windows Network Neighborhood.
 - Enter the Windows workgroup name being used by other workstations in the office. If you are setting up a new network, you can use any workgroup name you want, providing that you configure the Windows workstations so they belong to the same workgroup.
7. In the section labeled **WINS Support** select whether or not the Lotus Foundations server responds to WINS requests by clicking **Enable** or **Disable**.

If you select **Enabled** for the option above, specify the WINS server on the network in **WINS Server** section. If you want that Lotus Foundations server to act as the WINS server, leave the text box as is. If you want to use another server on the network to act as the WINS server, enter the IP address of that server.
8. Click **Save Changes**.
9. To ensure that the status of the file server has changed, select **Status** from the WebConfig menu. The Windows, Apple, and NFS File Server sections of the System Status screen should display the updated status.
 - It can take up to 15 seconds for file services to start, and during that time the status might read Error starting service.

Active server connections

The Active Connections section displays which server resources, such as opened files, are being used by client workstations.

To view the current active connections in Lotus Foundations:

1. Click **File Server** in the left-side menu of WebConfig. Click the **Active Connections** tab.
2. In the main window, you see a table that displays the following information:
 - **User Name** - indicates which user account is used to login to the network share.
 - **Machine Name** - indicates the workstation used to log into the network share.
 - **IP Address** - indicates the IP associated with the *Machine Name*.
 - **Connected Since** - indicated what time the share was connected to.
 - **Action** - provides the option of looking into further details of the connection . or deleting the connection.
3. If you click the edit icon  , you see a screen that displays the following information:
 - **User Name** - indicates which user account is used to login to the network share.
 - **Machine Name** - indicates the workstation used to log into the network share.
 - **Path** - indicates the path location of the share connection. If a file is in use, the actual file might display.
 - **Open Since** - indicates when the share was initially accessed.

Access control lists

An Access Control List (ACL) defines which permissions, or access rights, that each user or team has to a specific file or directory.

Administrators can modify a Lotus Foundations user or team's permissions, **Read Only**, **Read/Write**, or **No Permissions** on directories through the Lotus Foundations Permissions feature.

Setting a user's permissions

Follow these steps to set a user's permissions:

1. Click **File Server** in the left-side menu of WebConfig. Click the **Permissions** tab.
2. Scroll down the list of teams, admins, and users in the selection box and click the directory to which you want to assign permissions. Click **Show Permissions**.
3. The Modify File Permissions screen is displayed showing the current permissions for that directory.
4. Modify the user's permissions by selecting either the **Read Only**, **Read/Write**, or **No Permissions** radio button. Click the check mark button in **Include Subfolder(s)** if you want the same permission applied recursively, then click the save icon in the **Action** column.
5. If you want to add permissions, in the last row titled **Add**, select the folder from the drop-down, and click the green plus sign in the **Action** column.
6. To set all of the files and folders under the current directory back to the default permission value, click **Reset Folder Permissions**.
7. To set all of the files and folders under the current directory, including all sub-folder files back to the default permission value, click **Reset Tree Permissions**.

Setting a team's permissions

Follow these steps to set a team's permissions:

1. Click **File Server** in the left-side menu of WebConfig. Click the **Permissions** tab.
2. Scroll down the list of teams, admins, and users in the selection box and click on the directory of the team to whom you want to assign permissions. Click **Show Permissions**.
3. The Modify File Permissions screen is displayed, showing the current permissions for that directory.
4. Modify the team's permissions by selecting either the **Read Only**, **Read/Write**, or **No Permissions** radio button. Click the check mark button in **Include Subfolder(s)** if you want the same permission applied recursively, then click save icon in the **Action** column.
5. To view the permissions of all users assigned to that team, click the plus symbol to the left of the team name in the Modify File Permissions section. This expands the team list and show all users within that team and their permission levels.
6. If you want to add permissions, in the last row titled **Add**, select the folder from the drop-down, and click the green plus sign in the **Action** column.
7. To set all of the files and folders under the current directory back to the default permission value, click **Reset Folder Permissions**.
8. To set all of the files and folders under the current directory, including all sub-folder files back to the default permission value, click **Reset Tree Permissions**.

Setting permissions in Windows

Alternatively, you can configure file and folder permissions in Windows. Refer to the following links for further information:

How to Share and Set Permissions for Folders and Files Using Windows XP:

<http://www.microsoft.com/technet/prodtechnol/winxppro/maintain/filessharing.mspx>

File and Folder Permissions (Windows 2000):

<http://www.microsoft.com/technet/prodtechnol/windows2000serv/deploy/confeat/13w2kadc.mspx>

Disk quotas

Disk quota defines the maximum amount of hard disk space allowed for a user's files and email. The disk quota feature in Lotus Foundations helps administrators to set specific disk quotas for individual users.

For example, a user's disk quota value can be set to predetermined values such as small, medium, or large, to a specified value for that user, or you can choose not to have the user's disk usage subject to a quota.

Disk quotas pertain to a user's files and email data, which can each be configured separately. The ability to modify the quotas for files and email separately is unique to Lotus Foundations.

Setting default disk quota values

Follow these steps to set default disk quota values that can be used when assigning disks quotas to users:

1. Select **Quotas** from the left-side menu of WebConfig. The main Quota Setup screen is displayed.

The screenshot shows the 'Quota Setup' screen in the WebConfig console. On the left is a vertical menu with 'Quotas' highlighted. The main content area is titled 'Quota Setup' and contains three input fields for 'Default Small Quota Value', 'Default Medium Quota Value', and 'Default Large Quota Value', each followed by 'MB'. Below these fields are two buttons: 'Save Changes' and 'Cancel Changes'. Underneath are two tables. The first table is titled 'Teams Over Quota' and has columns for 'Team ID', 'Disk Space Used', and 'Status'. The second table is titled 'Users Over Quota' and has columns for 'User ID', 'Disk Space Used', and 'Status'. Both tables show '(No teams are over their quota.)' and '(No users are over their quota.)' respectively.

Figure 17. Quota Setup screen in the WebConfig console

2. Enter a **Default Small Quota Value**.
3. Enter a **Default Medium Quota Value**.
4. Enter a **Default Large Quota Value**. The maximum size that a disk quota value can be is 2 TB.
5. Click **Save Changes** to save the default quota values.

Setting individual user disk quotas

Follow these steps to define a user's disk quota:

1. Select **Users** from left-side menu of WebConfig. The main User Setup screen is displayed.
2. Click the **Users** tab. Click the appropriate user's edit action icon . The Modify User screen is displayed. There are two separate sections for quota setup. **Quota Value** is for the user's files and **Email Quota Value** is for the user's emails.
3. In each field, select a quota value from the drop-down list for that user. Your options are:

- **Unlimited** - no limit set for this user
 - **Specified...** - when selected, a text field opens that permits the user to specify the quota in MB.
4. The value set within quota setup can be used for both files and emails. Therefore, if you have set a quota value of 100 MB, you can assign 100 MB for files and 100 MB for email. The maximum size that a disk quota value can be is 2 TB.
 5. Click **Save Changes** to save the quota values for that user.

Quota limit

All disk quota limits on Lotus Foundations are enforced as hard limits. This means that administrators can only define an absolute maximum and not a soft limit for warnings to users. When a user's quota limit is reached, Lotus Foundations prevents that user from using any more space on the hard disks by preventing them from creating new files, editing existing files, or receiving emails.

User accounts with a quota over the limit cannot:

- Write to the disk anymore until some space is cleared.
- Login to Lotus Domino.
- Receive any new email.

When accounts have reached a quota, administrators:

- See a yellow warning light in the Quota section of the System Status screen informing them that there are users over their quota.
- Notice the user's Disk Space Used column on the User Setup screen reports something similar to: "4.1 MB / 1.5 MB (274 %)".
- See a list of user(s) over their quota on the Quota Setup screen.
- Receive an email report when the server's disks reach 90% full. Another notice is not sent unless the disk space drops below 85% usage and then rises again above 90%.

NT domain services

Configuring Lotus Foundations Domain Settings

The domain settings for Lotus Foundations are located in the File Server section in WebConfig.

Click **File Server** in the left side menu of WebConfig. The **Basic Setup** tab is the default view. The options for configuring domain settings are located in the **Windows File Server** drop-down box.

You have the following options:

- **Disabled** - disables Windows file sharing and domain services in Lotus Foundations.
- **NT Domain Controller** - configures the Lotus Foundations server as a domain controller.
- **NT Domain Member** - configures the Lotus Foundations server as a domain member.
- **Active Directory Member** - configures the Lotus Foundations server as a member of an Active Directory environment.
- **Stand Alone** - enables Windows file sharing services in Lotus Foundations and disable the domain settings.

See "*File services*" on page 36 for more information on the following topics:

- File services in stand alone mode
- Permissions
- Active connections

Note: Because different versions of Lotus Foundations can contain modifications to domain functionality, it is strongly recommended that Lotus Foundations servers acting as domain members or a domain controller are running the same version on each server.

What is a domain controller?

A domain controller provides authentication services to the rest of the computers on the network. It stores user account and security information in a central database for one domain. When a user logs on to a computer that is part of the domain, the domain controller authenticates the username and password against the information in the directory database.

Lotus Foundations can serve as a Windows domain controller for all the computers running Windows on the network. When this function is enabled, the Windows file server is set up as a domain controller and a domain name replaces the Windows workgroup.

The network domain name has nothing to do with the Internet domain name. They do not interact and are independent of each other.

Note: Do not use the same Internet domain name as your local network domain name.

Configuring the domain controller

Follow these steps to enable Lotus Foundations as a domain controller:

1. Click **File Server** in the left side menu of WebConfig. The File Server Setup screen is displayed.

| File Server Setup | |
|--|---|
| Basic Setup Permissions Active Connections | |
| File Virus Scanner: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| NFS file server: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Macintosh File Server: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| Windows File Server: | NT Domain Controller Machine Accounts |
| Windows Workgroup/Domain: | WORKGROUP |
| Domain Admin Team: | root Edit |
| Roaming Profiles: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| WINS Support: | <input checked="" type="radio"/> Enable <input type="radio"/> Disable |
| WINS Server: | Local server |

Save Changes | Cancel Changes

Figure 18. File Server Setup screen in the WebConfig console

2. For the **Windows File Server** drop-down box, select **NT Domain Controller**.
3. Enter a name in the **Windows Workgroup/Domain** field. This is the domain name once the domain controller is enabled. Avoid using the default name of WORKGROUP.

4. For **Domain Admin Team**, select any additional users to add to the *domain_admins* team. Members of this team have the exclusive ability to authenticate workstations to the Lotus Foundations domain.
5. The **Roaming Profiles** selection enables or disables roaming profiles for Windows workstations.
6. For **WINS Support**, select whether or not the Lotus Foundations server responds to Windows Internet Name Service (WINS) requests by clicking **Enable** or **Disable**.

If you select **Enabled** for the option above, specify the WINS server on the network in **WINS Server**. If you want that Lotus Foundations server to act as the WINS server, leave the text box as is. If you want to use another server on the network to act as the WINS server, enter the Internet Protocol (IP) address of that server.

7. Click **Save Changes**.

You need to set each Windows workstation's domain name to match this for Windows file and printer sharing to work properly.

What is a Windows NT domain member?

Lotus Foundations can become a member of a Windows NT domain, enabling Lotus Foundations to authenticate users using a pre-existing Windows NT domain controller rather than local passwords.

The Windows NT domain stores all user account and security information in a central database. When a user logs on to Lotus Foundations, the Windows NT domain authenticates the username and password against the information in the directory database. This means that you do not need to maintain a separate directory database for both Lotus Foundations and Windows systems. Lotus Foundations users can access their network files from both Windows and Lotus Foundations systems with the same username and password. All administration can be done with Windows NT.

Configuring the domain member

Follow these steps to enable Lotus Foundations as a domain member:

1. Click **File Server** in the left side menu of WebConfig. The File Server Setup page is displayed.
2. In the **Windows File Server** drop-down box, select **NT Domain Member**.
3. Enter the domain name in the **Windows Workgroup/Domain** field.
4. For **Domain Admin Username**, enter the username of a member of the *domain_admins* team on the Lotus Foundations domain controller. If you are authenticating to a Windows domain controller, enter a username belonging to the *domain_admins* group on the Windows server.
5. For **Domain Admin Password**, enter the corresponding password to the username you provided in the previous box.
6. For **WINS Support**, select whether or not the Lotus Foundations server responds to Windows Internet Name Service (WINS) requests by clicking **Enable** or **Disable**.

If you select **Enabled** for the option above, specify the WINS server on the network in the **WINS Server** field. If you want that Lotus Foundations server to act as the WINS server, leave the text box as is. If you want to use another server on the network to act as the WINS server, enter the Internet Protocol (IP) address of that server.

7. Click **Save Changes**.

Connecting the active directory member

Follow these steps to add the Lotus Foundations server as a member of an active directory environment:

1. Click **File Server** in the left side menu of WebConfig. The File Server Setup page is displayed.
2. In the **Windows File Server** drop-down box, select **Active Directory Member**.
3. Enter the domain name in the **Windows Workgroup/Domain** field.
4. For **Domain Admin Username**, enter the username of a member of the Domain Administrators group on the Windows server.

5. For **Domain Admin Password**, enter the corresponding password to the username you provided in the previous box.
6. For **WINS Support**, select whether or not the Lotus Foundations server responds to Windows Internet Name Service (WINS) requests by clicking **Enable** or **Disable**.
If you select **Enabled** for the option above, specify the WINS server on the network in the **WINS Server** field. If you want that Lotus Foundations server to act as the WINS server, leave the text box as is. If you want to use another server on the network to act as the WINS server, enter the Internet Protocol (IP) address of that server.
7. Click **Save Changes**.

Verifying server connectivity

After you have selected and configured a mode in Lotus Foundations, you can verify the status on the main System Status page of WebConfig in the **User Authentication Method** section.

If you have set Windows File Server to **Disabled**, you should see:

Table 4. User Authentication Message

| Section | Image | Message |
|-----------------------------|---|---|
| User Authentication Method: |  | Using normal password authentication. x of x user licenses available. |

If you have set Windows File Server to **NT Domain Controller**, you should see:

Table 5. User Authentication Message

| Section | Image | Message |
|-----------------------------|---|--|
| User Authentication Method: |  | Authenticating users for domain DOMAIN_NAME as a Windows NT domain controller. Using normal password authentication. x of x user licenses available. |

If you have set Windows File Server to **NT Domain Member**, you should see:

Table 6. User Authentication Message

| Section | Image | Message |
|-----------------------------|---|--|
| Windows Domain Membership: |  | Joined domain DOMAIN_NAME (SERVER_NAME/IP_ADDRESS) |
| User Authentication Method: |  | Using Windows domain DOMAIN_NAME via password server SERVER_NAME/IP_ADDRESS. x of x user licenses available. |

If you have set Windows File Server to **Stand Alone**, you should see:

Table 7. User Authentication Message

| Section | Image | Message |
|-----------------------------|---|---|
| User Authentication Method: |  | Using normal password authentication. x of x user licenses available. |

Monitoring machine accounts

Machine account monitoring is available in NT Domain Controller mode and lists all machine trust accounts of the current domain.

Click **File Server** in the left side menu of WebConfig, then click the **Machine Account** link.

The status of a machine trust accounts is displayed as one of the following:

- **Joining** - The machine is in the process of joining the current domain.
- **Joined** - The machine has already joined the domain, but no user is currently accessing the domain controller through that machine.
- **Active** - One or more users are currently accessing the domain controller through that machine.

If you want to remove a machine account from the list, click the delete icon . This can be used to clean up the list or remove domain access from a workstation. This comes into effect the next time that workstation attempts to log into the domain.

Importing domain users and groups

Note: Each account that is imported uses a license on the member server. If there are not enough licenses on the member server, you receive an error notice indicating that your license limit has been exceeded and accounts might not work correctly.

From a member server, you can import domain groups and users from the domain controller. This helps you to selectively choose which accounts you want to import and ensures that authentication and other domain related features are consistent across the network.

The Import Users section can be used for importing accounts using the pwdump2 utility or by manually entering the accounts syntactically. For more information, read “Import users from Windows” on page 32.

Follow these steps to import domain users and groups:

1. Click **Users** in the left side menu of WebConfig.
2. Click **Import Users**.
3. From the **Domain Controller Groups** and **Domain Controller Users** fields, highlight the accounts that you want to import to the member server and click **Import**.

Note: The only user account that cannot be imported is root.

4. Click **Save Changes**. A page displaying the imported items, along with other information is displayed.
 - **PWDUMP2 Generated Users** - Indicates which accounts have been imported using the pwdump2 utility. The information provided includes the user name of the account, along with the Lanman hash and MD5 hash strings.
 - **Syntactically Generated Users** - Indicates user accounts that have been manually entered into the Import Users section. The information provided is the user name of the account, the password for the account (in plain text), the full name, and the quota and quota type, if one has been assigned.
 - **Imported Domain Groups** - Indicates which groups you have specified to import to the member server. The information provided is the group name, the members of that group, and the quota and quota type, if one has been assigned. Group members who exist in the domain controller, but not in the domain member, are not displayed in the Members field.
 - **Imported Domain Users** - Indicates which users you have specified to import to the member server. The information provided is used as the user names, their passwords (in plain text), and the quota and quota type, if one has been assigned.
5. After you have verified all of the imported accounts, click **Save Changes**.

Authentication status

After a domain member server is connected to the domain controller and all of the desired accounts have been imported, you can verify the authentication status. In the **User** section of WebConfig, a new column labeled **Authenticate** is displayed and indicates whether an account is local or remote.

If the status indicates local, the account only exists on the member server. If the status indicates remote, the account exists on both the member server and the domain controller.

Note: If the same user account exists on both servers, prior to domain connectivity, the accounts synchronize and automatically use the authentication on the domain controller. After the accounts are synchronized, the status of the users that existed on both accounts changes from **local** to **remote**.

File mounting/drive mapping

After the domain controller is enabled, a user's folders can be mounted directly onto any domain workstation upon login. The shared folders of any team that the user belongs to can also be mounted.

For Users

To mount files or map drives for users, follow these steps:

1. Click **Users** in the left side menu of WebConfig.
2. Click the **Users** tab.
3. Click the edit icon  in the Action column for the appropriate user. The Modify User page is displayed.
4. From the drop-down menu in the **Automatically mount files as** field, select the drive as which the user's files should be mounted on the workstation. The default drive is X:.

Note: Ensure you choose a drive that does not conflict with drive already in use.

5. Click **Save Changes**.

This can also be done when the user is created.

For Teams

To mount files or map drives for teams, follow these steps:

1. Click **Users** in the left side menu of WebConfig.
2. Click the **Teams** tab.
3. Click the edit icon  in the Action column for the appropriate team. The Modify Team page is displayed.
4. From the drop-down menu in the **Automatically mount files as** field, select the drive as which the team's shared files should be mounted on the workstation. The default, **Disabled**, is to not mount the files at all. This ensures that there is no conflict between use of drive space.
5. Click **Save Changes**.

This can also be done when the team is created.

Joining Windows systems to a domain

All Microsoft Windows workstations need to authenticate to the domain once the domain controller is enabled. Authentication to the domain only works using a user account that belongs to the *domain_admins* team.

Once a Windows workstation has joined the domain, users can change their passwords using the standard Windows interface or from WebConfig.

Windows operating systems which are not officially supported for use with Lotus Foundations domain controllers are the following:

- Windows 95
- Windows 98
- Windows ME
- Windows Vista
- Windows Vista Home

For Windows NT

1. In Windows, select **Start** → **Settings** → **Control Panel**. The Control Panel window is displayed.
2. Select **Network** from the list. The Network window is displayed. Click the **Identification** tab.
3. Click **Change**. The Identification Changes window is displayed.
4. In the Member of section of the window, select **Domain**. Enter the name of the domain as entered in the **Windows Workgroup/Domain** field in the **Basic Setup** tab of the File Server Setup page of the WebConfig console.
5. Check the box for **Create a Computer Account in the Domain**. Enter a *domain_admins* username and the corresponding password.
6. Click **OK**. The Network window is displayed. Click **OK** again.
7. Reboot the workstation. The next time you log in to Windows, a drop-down box is displayed. Select the domain name (for example, MAINOFFICE) and a user account and password belonging to that domain.

For Windows 2000

1. In Windows, select **Start** → **Settings** → **Control Panel**. The Control Panel window is displayed.
2. Select **System** from the list. The System Properties window is displayed. Click the **Network Identification** tab.
3. Click **Properties**. The Identification Changes window is displayed.
4. In the Member of section of the window, select **Domain**. Enter the name of the domain as entered in the **Windows Workgroup/Domain** field in the **Basic Setup** tab on the File Server Setup page of the WebConfig console.
5. Click **OK**. The next time you log in to Windows, the login window has an additional **Domain** field.

For Windows XP Professional

1. In Windows, select **Start** → **Settings** → **Control Panel**. The Control Panel window is displayed. On the left menu bar under Control Panel, select Classic View if you are currently in Category View.
2. Select **System** from the list. The System Properties window is displayed. Click the **Computer Name** tab.
3. Click **Change...** The Computer Name Changes window is displayed.
4. In the Member of section of the window, select **Domain**. Enter the name of the domain as entered in the **Windows Workgroup/Domain** field in the **Basic Setup** tab on the File Server Setup page of the WebConfig console.
5. Click **OK**. The next time you log in to Windows, a drop-down box is displayed. Select the domain name (for example, MAINOFFICE) and a user account and password belonging to that domain.

Logon scripts

Logon scripts are supported through MS-DOS batch files found at `\\Servername\netlogon`. All scripts are called `USERNAME.bat`. These batch files call upon `_logon.bat`. If manual modifications are required, create a file called `_logon.bat`. All manual modifications should be made to `_logon.bat`, as `USERNAME.bat` is automatically generated and modifications are lost.

Automated drive mapping

You can automatically mount user folders and team folders through the selection of a drive mount in the Modify User, Add User, Modify Team, or Add Team setup pages. These drive mappings are done through the logon scripts. Note that any drives previously mounted are not automatically disconnected as Windows caches these drive connections.

Workstation administrative rights

Administrators can add users to the `domain_admins` team to give them workstation administrative rights to all computers running Windows on the network. Users have full control over workstation administration without giving them access to other server administrator functions. Adding users to the `domain_admins` team only gives them administrative rights over a Windows client if the Windows client is joined to the domain.

Giving users workstation administrative rights

1. Click **Users** in the left side menu of WebConfig.
2. Click the **Teams** tab, then click the edit icon  in the Action column for the `domain_admins` team. Add any users to the `domain_admins` team that you want to grant access to workstation administrative features. See “User & Team management” on page 29 for instructions on how to create a team.
3. The next time that user logs in to the domain, they have workstation administrative rights.

Lotus Foundations scalable services

Overview

Lotus Foundations scalable services are not intended to replace the functionality provided by Microsoft Windows domains. They are designed with the intention of making Lotus Foundations more scalable by centralizing the administration of a group of Lotus Foundations servers.

Scalable services employ a master-slave network model, enabling a single master server to centrally manage all users and licensing for multiple slave servers.

Lotus Foundations scalable services introduction

The needs and concerns of small to medium businesses can be best met with a single easy-to-use and easy-to-manage device. As organizations grow, they are generally required to expand their network services as additional load is placed on the single server. Scalable services are designed to facilitate the needs of growing organizations while still maintaining ease-of-use and capitalize on Lotus Foundations' ease-of-deployment. They introduce the ability for multiple Lotus Foundations servers to be deployed across an organization yet still provide centrally managed user and licensing. The hierarchical model allows for an organization to design their infrastructure to most efficiently deliver services based on the following:

- Number of employees
- Geographic expanse
- Actual usage of services and resources of the IT infrastructure

Lotus Foundations scalable services terminology

Table 8. Lotus Foundations scalable services terminology

| Term | Definition |
|---------------------------------|--|
| Login access | The Lotus Foundations server to which each team/user is assigned |
| Scalable services region | A group of Lotus Foundations servers configured to share scalable services-related information, such as master server, slave servers, teams, team members, and users; a Lotus Foundations server may be a member of one region at most |
| Scalable services master server | The sole administration point for a scalable services region |
| Scalable services slave server | Any Lotus Foundations server with the scalable services feature enabled and not acting as the scalable services master server |
| Scalable services node | Any Lotus Foundations server that is either a scalable services master or scalable services slave |
| Standalone server | Any Lotus Foundations server without scalable services enabled |

Features of Lotus Foundations scalable services

There are three main features of Lotus Foundations scalable services:

- User synchronization
- Domain Name Service (DNS) synchronization
- Scalable services licensing and user licenses

User synchronization

Lotus Foundations scalable services helps you centrally manage user and team information from the Lotus Foundations scalable services master server. The synchronization of users and team includes ALL user configuration information, including the following information:

- Username
- Password
- Full Name
- Team membership
- Administrative rights
- Point-to-Point Tunneling Protocol (PPTP) setting
- File Transfer Protocol (FTP) setting
- Drive mounting
- Disk quota

Synchronization occurs in a uni-directional manner. This means that all user configuration changes must be done on the master node. Any changes made to a synchronized user in the slave node is overwritten on the next synchronization. Any changes made to a user on the master replicates to the slave node on which the user has node access. If a previously existing user shares a name with a synchronized user, then the existing user's settings are overwritten. All team and user accounts exist on the master node. This enables all users to authenticate against the master.

The synchronization of a team automatically synchronizes all members of the team without having to specify the individual users. This includes teams that were members of the team transferred, as well as all of their users.

DNS Synchronization

This feature includes the ability to propagate workstation host names to the other nodes so that workstations and servers may be addressed by name across an Internet Protocol Security (IPSec) virtual private network (VPN) rather than just by Internet Protocol (IP) address.

The master accumulates lists of all host names from each slave, combines these lists with its own list of local host names, and distributes it to each of the slaves that has DNS Sync enabled. To resolve situations in which there are identical host names on different servers, DNS Sync sorts the list of host names such that hosts that are local to the current server are resolved first. That is, on a slave, local host names take priority over host names local to the master which, in turn, take priority over those on other slaves.

In the event that DNS records conflict (in other words, the same DNS name resolves to two different IP addresses that are on different nodes in the region), an entry from the local node preempts the remote node. An entry on the master preempts an entry from a remote slave. If two slaves have conflicting names, each one selects its own local name for itself, and the master selects one of the names to distribute to all the other machines. The name the master selects does not depend on the order in which the slaves have most recently synchronized, though it may depend on which slaves have supplied the conflicting names (for example, the original implementation resolves conflicts by selecting the slave with the host name that is first alphabetically). In order to guarantee that DNS entries are known and are consistent between scalable services servers, any DNS entry that has been explicitly set on the master takes precedence over any on a slave. This can only be overridden on a slave by explicitly setting a DNS entry that slave.

DNS Synchronization allows a scalable services region with multiple locations to use a single domain name across the entire region. By synchronizing with the master server on specified intervals, the slave servers also acquire the ability to recognize the region's domain and propagate it throughout the region. This makes it even easier to recognize all the servers by name, such as *master.domain.com*, *slave1.domain.com*, and *slave2.domain.com*, rather than having each node using their own domain name.

Scalable services licensing and user licensing

User license management is simplified with scalable services. One user license is automatically synchronized to each slave for each user (or team that has its own password) synchronized to that slave. This means that in a typical setup, the master server is purchased with sufficient user license so that each user/team has one and slave servers do not need to be purchased with any. The master scalable services node requires user licenses for each user in the region.

User accounts that are no longer being synchronized to the slaves are not automatically deleted (and hence may use a user license on the slave). This is not of great consequence because the number of user licenses a slave has allocated to it depends on the accounts that are being actively synchronized. That is, extra (old) accounts on the slave are locked out.

By using scalable services, you can convert the Lotus Foundations user licenses on the master server into network user licenses. You no longer need to worry about user licenses for any of the slave servers, as they will automatically inherit any required user licenses from the master server for all users controlled by the master server.

Lotus Foundations scalable services regions

With Lotus Foundations scalable services, a hierarchical structure is used to centralize the management of the Lotus Foundations servers. This is best understood as a single master-to-multiple slaves configuration. Each scalable services hierarchy is known as a region.

At the top of each scalable services region is the master server. The master server is responsible for the configuration and account synchronization throughout the scalable services region.

Each node in the region is a complete Lotus Foundations server within itself, capable of providing all the normal Lotus Foundations services. Scalable services augment the Lotus Foundations abilities by providing the capability to configure user data between all nodes of the region. This synchronization is possible across the local area network (Internet Protocol Security - IPSec) and across the virtual private network (TunnelVision) to address geographically diverse environments.

The following diagram shows a sample Lotus Foundations scalable services region.

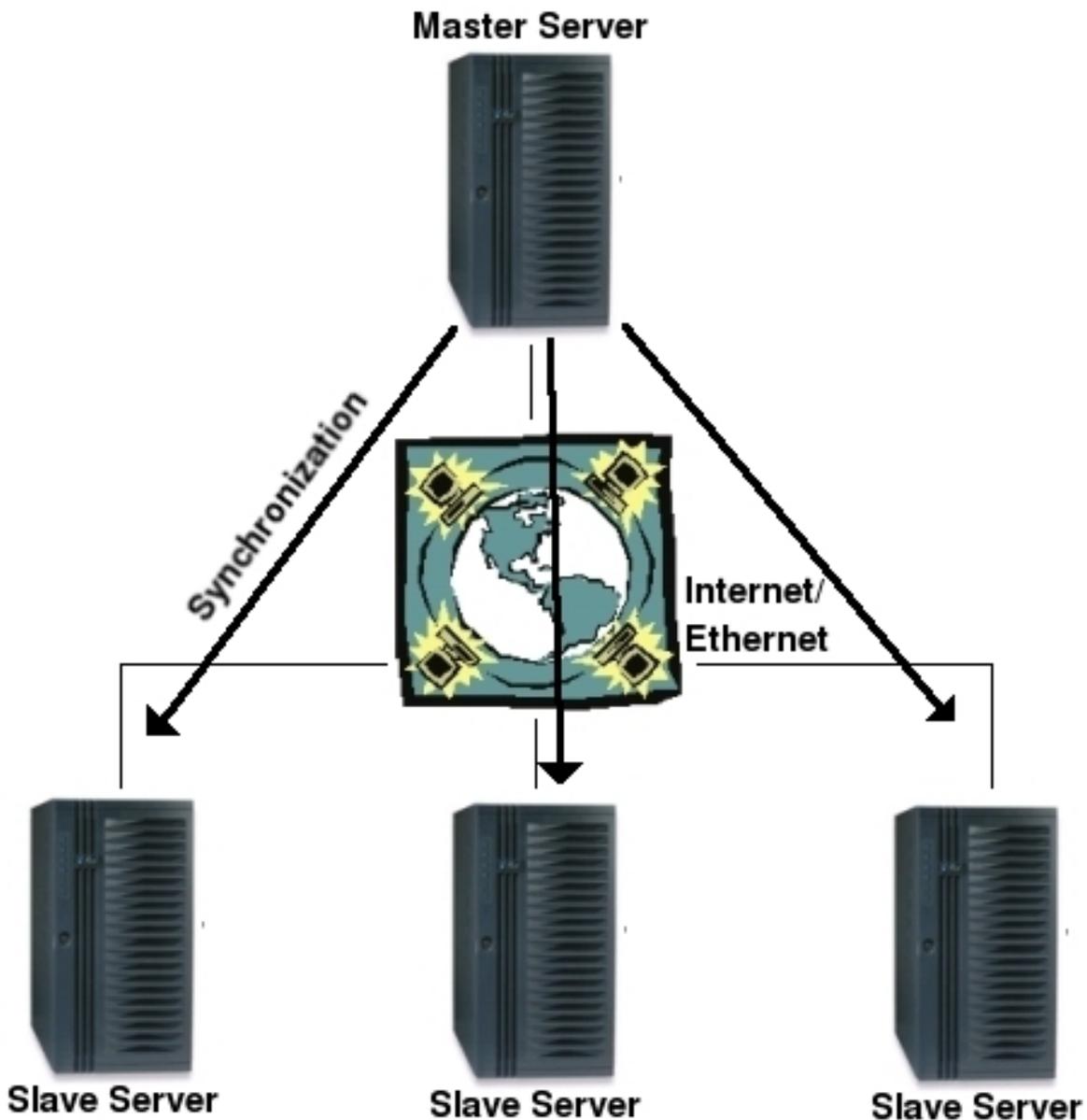


Figure 19. Sample scalable services region

Centralized Management and Administration

While Lotus Foundations already provides Web-based administration through WebConfig that is accessible remotely, the administration of users and teams across the entire network is not cohesive when deployed with standalone servers. User additions and modifications need to be manually replicated across the different Lotus Foundations servers to keep all the configurations synchronized.

Scalable services simplify this by centralizing the administration of the users and teams on the master server. Modifications to a user's configuration, such as a password change, are automatically synchronized to the slave servers.

Before enabling scalable services, an architectural plan should be constructed as to the layout of the IT network and the distribution of the users.

Setting up a scalable services region

If a Lotus Foundations server possesses a scalable services master or scalable services slave license, a link labeled **Scalable Services** is displayed in the left side menu of WebConfig.

On a standalone Lotus Foundations server that has a scalable services license, clicking **Scalable Services** in the left side menu of WebConfig opens a page containing the following table.

Figure 20. Scalable services Local Node Setup page

Table 9. Fields for the Local Node Setup page

| Local Node Setup Page Fields | Definition |
|--|---|
| Mode | Identifies the server as a standalone, master, or slave server |
| Scalable Services Region Name | Name of the scalable services region in which this server participates |
| Scalable Services Password/Re-enter Password | Password for the scalable services region |
| Sync Frequency | Frequency with which the master synchronizes user data and DNS data with the scalable services slaves; this field can only be configured on the master server |
| Master Node | IP address or (internal) host name for the master server; this field can only be configured on slave servers |

Configuring a master server

Selecting the **Mode** for the server as **Master** and clicking **Save Changes** refreshes the page to show the **Basic Setup** tab of the scalable services configuration page.

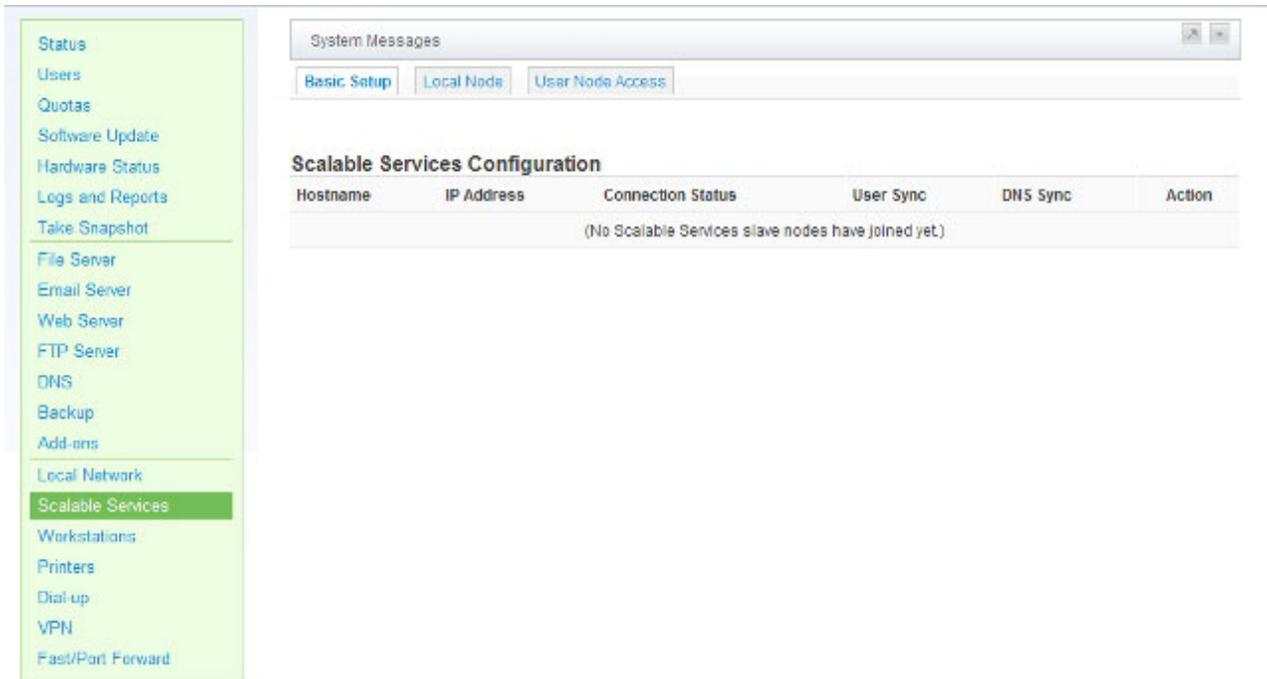


Figure 21. Basic Setup tab of the scalable services master server

The Scalable Services Configuration section of the **Basic Setup** tab displays the status of all slave servers in the region. As there are presently no slaves configured, this table is empty.

The **Local Node** tab displays the scalable services page described at the beginning of the *Setting up the scalable services region* section.

The **User Node Access** tab displays team node access and user node access. This page leads to configuration pages for user/team access and e-mail home servers.

Configuring a slave server

To configure a server as a slave server, follow these steps:

1. Click **Scalable Services** in the left side menu of WebConfig. A page is displayed that is similar to the page used when configuring the master server.
2. Select **Slave** for the **Mode** if it is not already selected. Fields not editable in standalone mode are now editable.

Figure 22. Slave server setup screen

3. For **Scalable Services Region Name**, type the name of the region you created when setting up the master server.
4. For the **Scalable Services Password** and **Re-enter Password** fields, type the password you created with the master server.
5. For **Master Node**, type the host name or IP address of the master server.
6. Click **Save Changes**.
7. Once you have clicked to save the slave server settings, two error messages are displayed in the Slave Node Status section of the Scalable Services page. The first message states the slaver server is not authorized to join the scalable services region. The second message states that DNS Sync requires the node to join the scalable services region. To remove the messages, return to the master server and authorize the slave server.

Authorizing a slave server on the master

The master must grant permission to each slave attempting to connect to the scalable services region.

After a slave has been configured and attempts to connect, a message is displayed in the Scalable Services Configuration section of the **Basic Setup** tab for **Scalable Services** with the machine information for the slave server that attempted to join the scalable services region.

| Basic Setup Local Node User Node Access | | | | | |
|---|-------------|-------------------|-----------|----------|--------|
| Scalable Services Configuration | | | | | |
| Hostname | IP Address | Connection Status | User Sync | DNS Sync | Action |
| enterprise7 | 9.3.186.138 | non-member | | | |

Figure 23. Master server with unauthorized slave server

1. On the master server, click **Scalable Services** in the left side menu of WebConfig.
2. In the Scalable Services Configuration section, click the edit icon in the Action column.
3. In the new page that opens, select **Member** for the **Standing** field.

Slave Node Status

User Sync: The master node has not authorized this node to join Scalable Services.

DNS Sync: DNS Sync requires that this node has joined the Scalable Services Region.

Modify Node

Hostname: enterprise7

IP Address: 9.3.186.138

Standing: Member Non-Member

Enable DNS Synchronization: Yes No

Node Users:

| Users | Node Login Access |
|--|---------------------|
| <ul style="list-style-type: none"> autoinstall backup clientinstallers daemon domain_admins domino ftp log netlogon notes notesbackup ns3-root printer_drivers root spam_scanner test1 test2 testteam webmaster webproxy | (No nodes selected) |

Figure 24. Modify Node page of the master server

- The **Hostname** and **IP Address** fields display the name and the IP address of the slave server requesting to join the scalable services region. For the **Standing** entry, select **Member** to add the slave server to the scalable services region.
- For the **Enable DNS Synchronization** entry, select **Yes** to enable the slave server to synchronize DNS information with the master server.
- In the **Users** section, click to highlight all the users you wish to assign to this node and click **Add**.

Slave Node Status

| | | |
|------------|-------------------------------------|---|
| User Sync: | <input checked="" type="checkbox"/> | The master node has not authorized this node to join Scalable Services. |
| DNS Sync: | <input type="checkbox"/> | DNS Sync requires that this node has joined the Scalable Services Region. |

Modify Node

| | | | |
|-----------------------------|---|---|--|
| Hostname: | enterprise7 | | |
| IP Address: | 9.3.186.138 | | |
| Standing: | <input checked="" type="radio"/> Member <input type="radio"/> Non-Member | | |
| Enable DNS Synchronization: | <input checked="" type="radio"/> Yes <input type="radio"/> No | | |
| Node Users: | <div style="display: flex; align-items: flex-start;"> <div style="border: 1px solid #ccc; padding: 5px; width: 200px;"> <p>Users</p> <ul style="list-style-type: none"> autoinstall backup clientinstallers daemon domain_admins domino ftp log netlogon notes notesbackup ns3-root printer_drivers root spam_scanner test2 testteam webmaster webproxy </div> <div style="margin-left: 10px;"> <p><input type="button" value="Add node user"/></p> <p><input type="button" value="Remove node user"/></p> </div> </div> | <div style="border: 1px solid #ccc; padding: 5px; width: 150px;"> <p>Node Login Access</p> <ul style="list-style-type: none"> test1 </div> | |

Figure 25. Adding users

- Click **Save Changes** to finish this configuration.
- After you have added the slave server to the scalable services region and authorized it, the update of the new slave server is displayed in the Scalable Services Configuration section of the **Basic Setup** tab of the **Scalable Services** page.

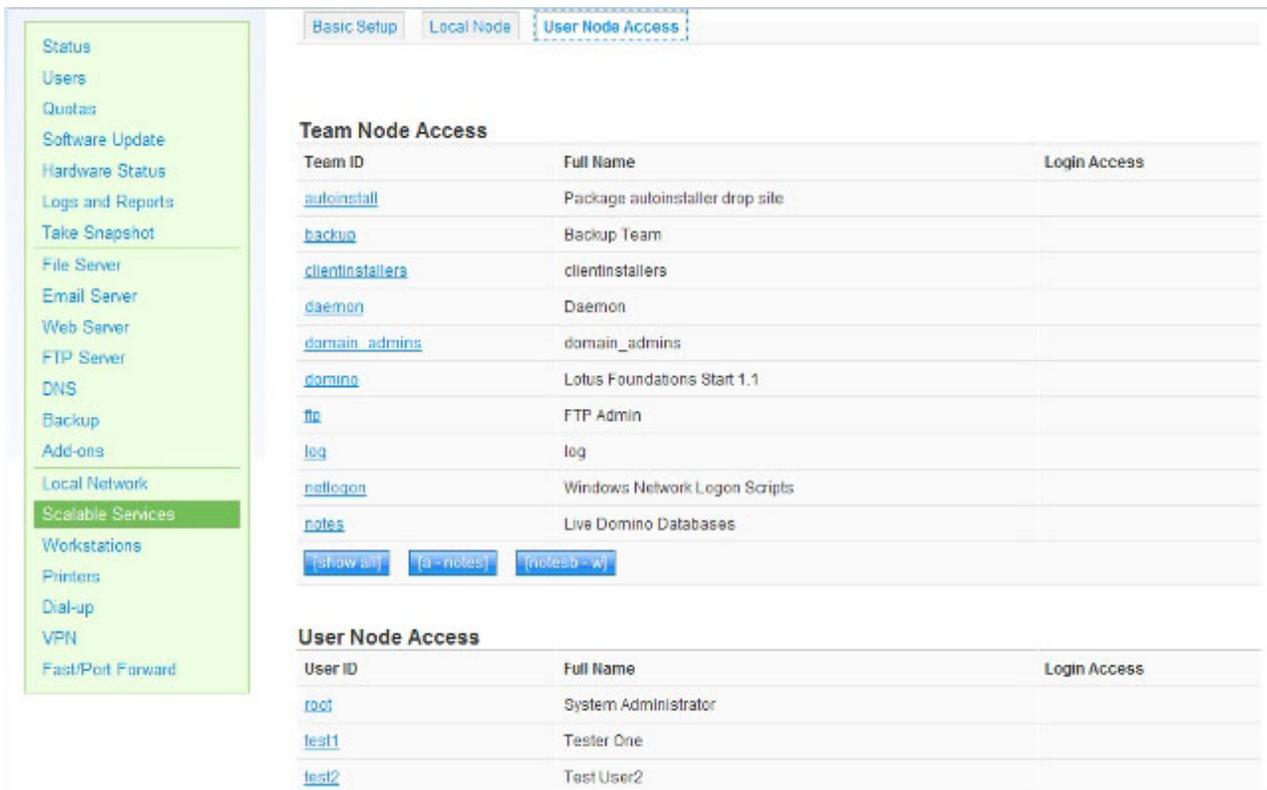
| Scalable Services Configuration | | | | | |
|---------------------------------|-------------|-------------------|-----------|----------|---|
| Hostname | IP Address | Connection Status | User Sync | DNS Sync | Action |
| enterprise7 | 9.3.186.138 | member | ✓ | ✓ |   |

Figure 26. Updated status page after authorizing a slave server to the scalable services region

Administering Users and Teams

You can manage all of your users and teams across the entire scalable services region from the master server with Lotus Foundations scalable services.

1. While logged into the master server, click **Scalable Services** in the left side menu of WebConfig. Then click the **User Node Access** tab in the Scalable Services page. The page lists the team nodes and user nodes for the scalable services region.
2. The **Team ID** and **User ID** list the teams and users in the scalable services region. To configure a team or user, click the name of the team or user you want to configure. The **Full Name** is a descriptive name for a team or user, and **Login Access** specifies the slave (if any) to which the account is synchronized. This setting can be configured in the setup page specific to the team or user.



| Team Node Access | | |
|----------------------------------|---------------------------------|-----------------------------|
| Team ID | Full Name | Login Access |
| autoinstall | Package autoinstaller drop site | |
| backup | Backup Team | |
| clientinstallers | clientinstallers | |
| daemon | Daemon | |
| domain_admins | domain_admins | |
| domino | Lotus Foundations Start 1.1 | |
| ftp | FTP Admin | |
| log | log | |
| netlogon | Windows Network Logon Scripts | |
| notes | Live Domino Databases | |
| [show all] | [a - notes] | [notes - w] |

| User Node Access | | |
|-----------------------|----------------------|--------------|
| User ID | Full Name | Login Access |
| root | System Administrator | |
| test1 | Tester One | |
| test2 | Test User2 | |

Figure 27. User Node Access page

3. Note the team named `NS3-region name`. This is automatically created and is known as the NS3 Team.

The scalable services team

Enabling Lotus Foundations scalable services prompts the system to create a new team named after the scalable services region. This team is password protected with the scalable services password and must exist for scalable services to function properly. Modifying, renaming, or deleting this team is not recommended while scalable services are enabled as unexpected behavior may occur. If the team is deleted or renamed, it is automatically recreated.

Lotus Foundations scalable services frequently asked questions

Some frequently asked questions about Lotus Foundations scalable services are listed below.

1. Are administrator accounts on the master server synchronized to the slave server(s)?

Like normal teams and users, you must specify the accounts that are synchronized. This includes administrator accounts.

2. What happens to my pre-existing team/user accounts on a machine that I change from a standalone machine to a scalable services slave server?

The team/user accounts still exist. If similarly named accounts exist on the master (and the master has been configured to synchronize them), their account information (such as the password, full name, and so on) are overwritten, but none of the data on disk is lost.

3. I have two Lotus Foundations servers that I have been using independently. I wish to combine them into an scalable services region, but they each have a number of unique team/user accounts. How can I easily merge their team/user accounts and set up my scalable services region?

The Export/Import User feature is useful for this kind of procedure. Unfortunately, it only exports/imports the username, full name, and password. If you are willing to set up your scalable services master with default values, use this feature.

Alternatively, you can follow a more thorough but time-consuming approach by configuring one machine as the master and another as the slave. Set up synchronization for users to synchronize everything to the slave, then switch their roles after the initial synchronization (make them standalone servers first) and repeat the process. As an example, if you have Server A and Server B, set Server A to master, Server B to slave, and then synchronize them. Next, change both servers to standalone mode. Finally, make Server A the slave and Server B the master. Following the subsequent synchronization, both servers contain an identical list of team/user accounts. This process can be extended to build up a complete list of team/user accounts on a server that you want to become an scalable services master server.

4. I deleted a team/user on the master server (or stopped synchronizing a team/user to a particular slave server), but that team/user still exists on the slave server. Why is that?

This is intentional so that data stored in the team/user's directory on the slave server is not automatically deleted.

5. Why can't a scalable services slave server also be a domain member?

This is intentional so as to avoid a host of problems related to conflicts arising between domains and scalable services regions. Basically, allowing a server to be both a domain member and a scalable services slave gives it two independent channels to create user accounts (one through Samba Pass Thru Authentication and another through scalable services).

Print service

Lotus Foundation print services

You can connect any type of printer that users are sharing on the internal network to the parallel printer port of a Lotus Foundations Start server. Lotus Foundations Start does not support the bi-directional mode of parallel devices; it can send output to printers but cannot read detailed status information. This means that any special print manager and status monitor software on your workstation should be disabled.

Lotus Foundations supports network printing. This helps you to manage the print queues through Lotus Foundations directly for multiple network-enabled printers. The printer queues are accessible through Internet Printing Protocol (IPP), and standard Windows network printing. Lotus Foundations also enables aliased printing queues.

The administrator or installer must provide the appropriate drivers for the specified printer at the workstation.

Lotus Foundations supports parallel port printers and a range of local USB-based printers. Print services do not support green-enabled printers that shut themselves off when there is inactivity on the port.

Configuring local print services

Before you can print on a printer connected to your Lotus Foundations server, you must configure Lotus Foundations for printing.

1. Click **Printers** in the left side menu of WebConfig. The Print Setup page is displayed. Lotus Foundations lists all the available printers.
2. For **Printing Services**, select **Enable** or **Disable**. You are not able to print with the printers connected to your server unless you enable printing services.
3. Click **Save Changes**. It takes approximately five seconds to detect connected printers. Printers are not displayed in the list immediately after clicking **Save Changes**.

Configuring your workstation

Follow these steps to configure a printer for your workstation:

Note: Driver installations can vary according to each printer and manufacturer. The following instructions are provided as a basic guideline. For more information, refer the printer manufacturer's installation guide.

1. Access the Lotus Foundations server file share. This can be done through Microsoft Windows Network or by clicking **Start** → **Run** and typing in either `\\server_ip` or `\\server_hostname`. A window is displayed that shows the network file and print services to which you have access.
2. Right-click the printer icon to which you want to connect and click **Connect**.
3. If the required driver is not detected as already installed, a print installation warning is displayed. Click **Yes** to continue.
4. Select the printer in the list provided and click **OK**. If your printer is not listed, click **Have Disk** and point to the driver provided by your printer's manufacturer.
5. Enter a name for the printer and click **Next**. If this is the only printer that the workstation is communicating with, it assumes that this printer is the default.
6. Indicate whether or not you want to print a test page and click **OK**.

Configuring network printers

1. Click **Printers** in the left side menu of WebConfig.
2. If **Printing Service** is disabled, select **Enable** and click **Save Changes**.
3. Click **Add Network Printer**.
4. Fill in details pertaining to the network printer to be added.
5. Click **Save Changes** to add the network printer.
6. Permit Lotus Foundations to probe the address for printer information, and click **Printers** in the left menu. Once the printer has been found, it displays the printer information.

Other network printing

If you are trying to configure network printing where the printer is not physically connected to a Lotus Foundations server, perform these steps:

1. In Windows, go to Printers & Faxes, click **Add a Printer** and select **A network printer, or a printer attached to another computer** on the second screen of the Add Printer Wizard.
2. Choose **Connect to this printer**, and type in the address and name of the printer; for example, `http://printer_ip:631/printer`
3. Click **Next**. Windows warns you about installing drivers from an untrusted source. It then states that it cannot find drivers for the given printer. Lotus Foundations does not keep a repository of printers to maintain its small operating size.
4. Select the type of printer, or download the driver from the printer's Web site.
5. Select whether or not you want this to be your default printer.

You should now be configured to print to the networked printer directly through Lotus Foundations. You can configure printing services through Linux and Mac workstations.

Performing printing queue tasks

Creating an aliased printer queue

1. Click **Printers** in the left side menu of WebConfig.
2. Click **Add Printer Alias...**
3. Enter the alias to apply to a particular printer.
4. Click **Save Changes** to create the alias.

Email services

Configuring email services

The **Email Server** section is divided into several tabbed sections that enable you to effectively manage all of the email services offered in Lotus Foundations Start.

Summary tab

The **Summary** tab displays a list of services, indicates status, and provides additional comments where necessary.

The options displayed are:

- **POP3 Server** - A system that receives a user's email messages and stores them in the user's mailbox. When a user's email client checks for new email, it communicates with the POP3 server, which ensures proper user authentication and delivery of email to the user's email client. POP3 is the most commonly used email delivery protocol.
 - **POP3/SSL Support** - This is the secure POP3 server. The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- **Internet Message Access Protocol (IMAP) Server** - An advanced system that is similar to POP3. Because IMAP is relatively new, not all email clients support it. IMAP offers superior user authentication and allows users to store their email on a server instead of downloading messages to a workstation (as is the case with POP3). This enables users to check their email from various workstations and lets them see a complete list of the emails kept in their folders.
 - **IMAP/SSL Support** - This is the secure IMAP server. The Secure Sockets Layer (SSL) is a commonly-used protocol for managing the security of a message transmission on the Internet.
- **SMTP Server** - An email delivery system. When you send an email, the SMTP server takes this message from the email client and delivers the message to the recipient's POP3 server. If the ISP forces you to use a specific SMTP server, Lotus Foundations can deliver to that server rather than directly to the destination servers. This is known as a 'smarthost'.

- **Virus scan** - Scans all outgoing and incoming email for viruses. If a virus is found, it is immediately removed from the email. A warning is then sent to the sender and all recipients along with the original, but virus-free, message. You must buy the Lotus Foundations AntiVirus license for Lotus Foundations for this feature to be enabled.
- **Spam scan** - Scans all incoming email for possible spam. If spam is detected, it categorizes the email as either probable or definite spam and enables you to choose what to do with the email including marking it, moving it to a spam folder, or deleting it.
- **RBL** - Sets the level of real-time blacklist (RBL) spam protection that the server uses. "No RBL" enables all email into the system without doing any checks on the sources. "Medium RBL" blocks all email originating from known spam sources. "Strong RBL" blocks email from known spam sources and spam relay servers and dialup accounts.
- **SMTP Authentication** - Enables remote users to send email through the Lotus Foundations server, preventing the need for the email setting to be modified every time a user changes locations. Lotus Foundations user account information must be provided within the email client settings for this feature to work.
- **Smarthosting** - Enables the SMTP server to route email to an intermediate server rather than directly to the user's email server. This requires SMTP authentication.
- **Attachment filter** - Enables Lotus Foundations to filter incoming emails that contain file attachments. The filtering can be done based on specified document extension types and specific users can be exempt from individual extension types.
- **Allowed relays** - IP addresses or domain names can be added to enable for email relaying from those specified locations.

Features handled by IBM Lotus Domino

The following features are handled by the Lotus Domino server that is integrated with Lotus Foundations Start:

- SMTP
- POP3
- POP3/SSL Server
- IMAP
- IMAP/SSL Server

Servers tab

The **Servers** tab enables you to control the various email features in Lotus Foundations. The options are as follows:

1. SMTP (mail delivery) server

- **Enable** - Enables the SMTP server and enables any computer on the internal network or on the Internet to send email using the Lotus Foundations server as an email server. Messages from computers on the Internet are accepted only if their destination is the local domain hosted by the Lotus Foundations server. (This prevents the server and Internet bandwidth from being used to send unsolicited emails).
- **Only Trusted Hosts** - Enables the SMTP server and enables internal users and users connected to the internal network through a VPN to send email using the Lotus Foundations server as their mail server.
- **Disable** - Disables the SMTP server completely.

2. POP3 (mail reader) server

- **Enable** - Enables the POP3 server and enables any computer on the internal network or on the Internet to access the POP3 mailbox. Select **Enable** only if you have users who access their email from outside of the office.

- **Only Trusted Hosts** - Enables the POP3 server and enables internal users to access the POP3 mailbox.
 - **Disable** - Disables the POP3 server.
3. **POP3/SSL (secure mail reader) server**
- **Enable** - Enables incoming secure POP3 connections from anywhere. This means that your users could download their email from anywhere on the Internet.
 - **Only Trusted Hosts** - Enables incoming secure POP3 connections only from the local network, and not from the internet.
 - **Disable** - Disables the secure POP3 server.
4. **IMAP (advanced mail reader) server**
- **Enable** - Enables incoming IMAP connections from anywhere. This means that your users could read their email from anywhere on the Internet.
 - **Only Trusted Hosts** - Enables incoming IMAP connections only from the local network, and not from the internet.
 - **Disable** - Disables the IMAP server.
5. **IMAP/SSL (secure advanced mail reader) server**
- **Enable** - Enables incoming secure IMAP connections from anywhere. This means that your users could read their email from anywhere on the Internet.
 - **Only Trusted Hosts** - Enables incoming secure IMAP connections only from the local network, and not from the internet.
 - **Disable** - Disables the secure IMAP server.
6. **Webmail Server**
- **Enable** - Enables incoming web requests from anywhere.
 - **Only Trusted Hosts** - Enables incoming web requests only from the local network and not from the Internet.
 - **Disable** - Disables Domino Web Access.
7. **LDAP directory server**
- Note:** These radio buttons are disabled when running Lotus Foundations Start.
- **Enable** - Enables the LDAP server, which answers directory queries. The LDAP directory is automatically populated with the names and email addresses of all users configured on the Lotus Foundations server.
 - **Disable** - Disables the LDAP server completely.
8. **Mail Domain**
- Displays only when Domino is disabled.
 - **Lotus Notes:** Enable or Only Trusted Hosts.
9. **SMTP Authentication**
- **Enable** - Enables the email server to be used as an SMTP gateway for remote Lotus Foundations users.
 - **Disable** - Disables the SMTP Authentication service.
10. **Reject Unknown Users**
- **Enable** - Blocks incoming emails containing users that do not exist on the Lotus Foundations server.
 - **Disable** - Enables incoming emails containing users that do not exist on the Lotus Foundations server. .
11. **Transport Layer Security (TLS) for Incoming Connections**
- **Enforce** - Enforces the requirement for inbound email to use a cryptic data transmission using the TLS protocol.
 - **Optional** - Disables the inbound cryptic data transmission using the TLS protocol.

12. **TLS for Outgoing Connections**
 - **Enforce** - Enforces the requirement for outbound mail to use a cryptic data transmission using the TLS protocol.
 - **Optional** - Disables outbound cryptic data transmission using the TLS protocol.
13. **Number of Incoming SMTP Connections**

Enter the number of incoming SMTP connections that you want to permitted at once.
14. **Email Size Limit in MB**

Enter the number limit for the size of incoming email messages. 25 MB is the default. It is recommended you do not go above 50 MB.
15. **Minutes Between Remote POP Mailbox Checks**

Enter the number of minutes that the server waits between checks for remote POP email messages.
16. **ISP's SMTP Server**

If the ISP forces you to use a specific SMTP server, enter that server's name.
17. **ISP's SMTP Port**

If the ISP forces you to use an SMTP port that is not the standard Port 25, input the port here.
18. **ISP's SMTP Username**

Enter the ISP login username if required.
19. **ISP's SMTP Password**

Enter your ISP login password if required.
20. Click **Save Changes**.

Filters tab

The **Filters** tab enables you to control the email filter feature in Lotus Foundations. The following options are available:

1. **Mail Virus Scanner**
 - **All Emails** - Scans all inbound and outbound email.
 - **Inbound Only** - Scans inbound email that targets local users only.
 - **Disabled** - Disables email virus scanning.
2. **RBL (spam blocker)**
 - **Strong RBL** - Blocks known spam servers and spam relay servers. Strong RBL blocks all spam email, but might also block other email. Senders receive a message if their email is blocked.
 - **Medium RBL** - Blocks known spam servers. Medium RBL blocks most spam email.
 - **No RBL** - Disables RBL spam protection.
3. **Mail Spam Scanner**
 - **Enable** - Enables email spam scanning. By clicking **Enable** the box expands to include the option to choose from the options in **Definite Spam Categories**.
 - **Disable** - Disables email spam scanning.

For more detailed information on using the spam scanning features in Lotus Foundations, refer to "Spam scanner" on page 142.
4. **Attachment filter**
 - **Enable** - Enables the attachment filter.
 - **Disable** - Disables the attachment filter.

The attachments file types that you want filtered and the users who you want excluded from filtering rules, can be defined in the **Attachment Extensions** section under the **Advanced Filtering** tab.

Monitoring tab

The **Monitoring** tab enables you to view email statistics and run email queries in Lotus Foundations. The following options are available:

Email Statistics

1. Active Queue

- **Trusted** - The number of emails sent from the internal trusted network that are pending delivery.
- **Untrusted** - The number of emails sent from the untrusted network which are pending delivery.

2. Waiting Queue

- **Trusted** - The number of emails sent from the trusted network which could not be delivered right away due to an error.
- **Untrusted** - The number of emails sent from the untrusted network which could not be delivered right away due to an error.

3. All Queues

- The total number of emails in all queues.

For each queue, you can choose to resend all the items by selecting the resend icon  or delete all the items in each queue by selecting the delete icon .

Query Parameters

Using the query parameters you can query the queue for emails based on the information you need. You create a query by filling in any of the following:

1. Select what you want to view in your query results:
 - Size
 - Date
 - Sender
 - Recipient
 - IP address
2. Select the minimum email size (in kbytes).
3. Select the minimum time in queue (in minutes).
4. Enter a specific sender's email address.
5. Enter a specific recipient's email address.
6. Click **Start New Query**.

When you start a new query, it switches you to a page that lets you view the query results. If you leave this page you can get back to the query results by clicking **View Query Results**. If you want to refine your query based on the query you just ran, click **Run against existing query** and the query you just ran is refined based on the parameters you changed. By clicking this button you are not searching the queue for new emails, you are only eliminating emails from the query. If you want the latest data from the queue you have to click **Start new query** again.

Example Query

For example, you might have a user, jdoe, that when she sends an email with a attachment to root, it does not get delivered. To query and see the emails, you would follow these steps from the **Monitoring** tab:

1. Check to see if there are any emails stuck in the queue in the **Waiting Queue** row in the Email Statistics section. As an example, you see that there are 10 emails in the **Trusted** row in the waiting queue.
2. In order to find out which of those emails are from the user to root that have an attachment, fill out the query form in the Query Parameters section by following these steps:
 - a. For **Fields to display**, click the **Size**, **Date**, **Sender**, and **Recipient** check boxes.
 - b. Enter a size in the **Minimum email size (in kbytes)** field. For example, 10.
 - c. Enter a time in the **Minimum time in queue (in minutes)** field. For example, 1.
 - d. Enter a user name in the **From email address** field. It does not have to be the entire email address. A search is done for what is provided in the field, so if it appears anywhere in a 'from' email address, it is returned in the query. For example doe.
 - e. Enter a user name in the **To email address** field. The same rules apply as used in the **From email address** field. For example, root.
3. Click **Start New Query**.
4. After the query is complete, the view switches to a Query Results section. In the Query Results section, the following items are displayed:

| Column | Description |
|---------------|--|
| Queue Id | This is the individual identifier of the email. This helps tell two emails apart. This is usually used internally for your own email purposes, but it also might help a technical support group to have the value. |
| Queue type | There are five queue types. <ul style="list-style-type: none"> • active: Being delivered • incoming: Just received • deferred: There was an error processing • hold: The email is being held by the administrator • corrupt: The email received has been corrupted |
| Queue Source | There are two values: <ul style="list-style-type: none"> • trusted: the email is from the internal network • untrusted: The email is coming from the internet |
| Size (kbytes) | The size of the email including email headers. |
| Date | The date it was received. |
| From | The original sender of the email. |
| To | The recipient of the email. |
| IP | The IP address of the last place the email came from. This can be confusing, but emails are bounced around the internet so this is the email of the final gateway which sent you the email. |
| Action | There are three actions you can take: <ul style="list-style-type: none">  - View all the fields for a particular email, even if they weren't included in the query  - Resend an email  - Delete an email |

Addressing tab

The **Addressing** tab enables you to manage virtual email domains, mailing lists and email aliases.

Available Mail Domains

This section lists the all of the domains hosted on the server and enables you to specify which users can use the domain for email purposes.

By default, all users on the server have access to all of the domains. If no users are added, the server assumes that all users have access.

Should you want to modify user access to a specific domain, follow these steps:

1. Click on the virtual domain action button.
2. In the Modify Virtual Domain box, highlight the users you want to add for this domain and click **Add >>**.
3. Click **Save Changes**.

Mailing list

The Mailing List section enables you to indicate which virtual domain on the server responds to, with respect to team mailing lists.

A team mailing list is first created in the main User Setup section of WebConfig.

In the Mailing List section, you should see that team name with a Responding Domain which should be the main Lotus Foundations domain.

To enable this mailing list to use a specific virtual domain:

1. Click the action button for the mailing list team.
2. In the Modify Mailing List Domain box, use the drop-down section to select the virtual domain you want to use.
3. Click **Save Changes**.

Advanced Filtering tab

The **Advanced Filtering** tab enables you to specify filter criteria, specifically regarding domains and attachment types. For example, you can configure a filter so domains that offer certain types of content are blocked or block file type attachments in email messages that could pose a liability to the business.

Add new filter

- **Filter criteria** - This option enables you to indicate what email you want to filter by email address, individual IP address, IP address range or domain name. Options are:
 - **Email address** - For example, username@example.com
 - **Domain name** - For example, example.com
 - **IP address** - For example, 192.168.0.1
 - **IP address range** - For example, 192.168.0.1/24

If you enter a domain name, you can use wildcards. For example *.example.com is an acceptable entry.

- **Relay** - This option enables you to indicate if you want this entry to be used as a relay. Setting the option to **Yes** permits email from that location to pass through the server's SMTP gateway without authentication. This option can be used alongside SMTP authentication or on its own.

- **Spam blacklist/whitelist** - Specify whether the item should be whitelisted or blacklisted. Whitelisted items always take precedence over blacklisted items.

Add new attachment filter

This section enables you to specify which extension to add to the list for filtering. The extension cannot start with a period. For example, .exe is not valid but exe and tar.gz are valid entries. Wild cards can be used in the name. For example, tar.* is a valid entry.

- **Attachment extension** - This option enables you to specify file types that are not permitted in incoming emails.
- **Exempted users** - This option enables you to select the users for which the individually specified filter rule does not apply.

Email DNS configuration

Although email services are functional after the administrator enables the appropriate email servers, the email delivery DNS records must be configured before users can send email to and receive email from outside of the internal network.

In the scenario that an email message is sent to johndoe@example.com, the message is downloaded to the SMTP server, which needs to know the IP address of example.com to deliver the message. The SMTP server consults the root DNS server on the Internet and through a series of queries is eventually pointed to the DNS server that stores the names and IP numbers of the hosts in example.com.

DNS Resolution

It is vital that your DNS server, which maintains information about the domain, is set up correctly. DNS resolution service can be provided by Lotus Foundations, or it can be provided by another DNS server maintained by you or by an ISP. If DNS resolution is provided by an ISP and you want Lotus Foundations to receive all emails for the domain, then make sure that you request the following from the ISP:

Mail exchanger records (MX) records for your domain should be pointed to your Lotus Foundations Start server's public IP address, that is, the address typically assigned to the eth1 interface.

If DNS resolution is provided by Lotus Foundations, make sure that the public IP address is registered with a proper domain name registrar as your domain DNS host.

Note: For Lotus Foundations Start to function properly as an email server for global email delivery, you must have a static IP address or use Dynamic DNS.

Configuring Lotus Foundations as a DNS server

To properly configure Lotus Foundations as a DNS server, follow these steps:

1. Click **Local Network** in the left-side menu in WebConfig. The Local Network Options screen is displayed.

Local Network Setup

| | | |
|---|--|----------------|
| Basic Setup | DHCP Server Options | Advanced Setup |
| Host Name: | egg5 | |
| Domain Name: | karen5.com | |
| Display the system status page for non-admin users: | <input checked="" type="radio"/> Yes <input type="radio"/> No | |
| LDAP directory server: | <input type="radio"/> Enable <input type="radio"/> Disable | |
| Rsync Server: | <input type="radio"/> Enable <input checked="" type="radio"/> Only Trusted Hosts <input type="radio"/> Disable | |
| Act as Public DNS Server: | <input checked="" type="radio"/> Yes <input type="radio"/> No <input type="radio"/> Dynamic | |
| Run DHCP Server on: | <input type="checkbox"/> eth0 | |
| SNMP Server (read only): | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |
| SNMP community name: | <input type="text" value="public"/> | |
| NIS Server: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable | |
| Restrict outgoing connections: | <input type="radio"/> Yes <input checked="" type="radio"/> No | |
| NTP Server: | <input type="radio"/> Enable <input checked="" type="radio"/> Only Trusted Hosts <input type="radio"/> Disable | |
| System Date and Time (from Internet): | 2/5/09 3:47:35 PM | |
| Adjust Time Zone: | <input type="text" value="GMT-6"/> (detected: GMT-6) Activate now | |

Figure 28. Configuring the DNS server

2. In the **Act as Public DNS Server** field, select **Yes**.
3. Click **Save Changes**.

Email client configuration

If Lotus Notes is being used as the email client, it is configured as part of the one-click deployment.

Although there are many different email clients available, the configuration of most clients is similar. The exact configuration of the email client depends on how you want the email delivery to be configured. The two most common configurations are listed in the following section. Configure the email client according to the configuration that resembles the email setup.

General setup

If the email is hosted on an ISP's email server:

All users in the office have their own email address and mailbox hosted on the ISP's server. The ISP supplies you with the name of the POP3 or IMAP server where the email has to be retrieved and with the address for the SMTP email delivery server. Enter this address into the appropriate field during the configuration of the email client.

Using the Lotus Foundations server as an SMTP server, even if the email is hosted by an ISP has its advantages, especially if you often send large messages or if there is a slow internet connection. The

email client may be tied up for minutes or even hours if a large email message is sent to an ISP's SMTP server. If the Lotus Foundations server is used as an SMTP server, large files are quickly transferred over the high-speed LAN. Although a file is then slowly transferred over the internet connection; the email client is free to perform other tasks.

Enter the following information when configuring the email client:

- For the SMTP server, enter the IP address or host name provided to you by the ISP. Alternatively, use the Lotus Foundations server as the SMTP server and enter the IP address or host name of the Lotus Foundations-powered server.
- For the POP3 or IMAP server, enter the IP address or host name provided to you by the ISP.
- For the POP3 or IMAP mailbox name, enter the first part of the email address. For example, if the email address is johndoe@example.com, enter johndoe.
- For the POP3 or IMAP password, enter the password provided to you by your ISP.

If the email is hosted on the Lotus Foundations server:

Enter the following information when configuring the email client:

- For the SMTP server, enter the internal IP (Eth0) address or host name of the Lotus Foundations server. You do not need to enter the domain name.
- For the POP3 or IMAP server, enter the internal IP (Eth0) address or host name of the Lotus Foundations server.
- For the POP3 or IMAP mailbox name, enter the Lotus Foundations username.
- For the POP3 or IMAP password, enter the Lotus Foundations password.

LDAP setup

Lotus Foundations has a built-in Lightweight Directory Access Protocol (LDAP) server, which provides a directory of user names and email addresses. It is automatically populated with names and email addresses of all Lotus Foundations users. Most email clients support access to read-only LDAP servers.

Configuring LDAP in Microsoft Outlook

To configure an Outlook XP client to user the Lotus Foundations LDAP service, follow these steps:

1. Open Microsoft Outlook. From the main menu, select **Tools** → **Accounts**. The Internet Accounts screen is displayed.
2. Select **Add** → **Directory Service**. The Internet Connection Wizard is displayed:
3. In the **Internet directory (LDAP) server** field, enter the name or IP address of the Lotus Foundations server.
4. Click **Next**.
5. Indicate whether or not you want the email client to check addresses using the LDAP directory. If this option is selected, the user can enter partial email addresses when sending emails. Outlook automatically finds the closest match in the LDAP directory and enter the correct email address.
6. Click **Next**.
7. Click **Finish**. The Internet Accounts screen is displayed again.
8. Click **Properties**.
9. Select the **Advanced** tab. The Advanced screen is displayed.
10. In the **Search Base** field, enter the following, replacing EXAMPLE.COM with the Internet domain name hosted on the Lotus Foundations server.
o=EXAMPLE.COM
11. Click **OK**. The Internet Accounts screen is displayed again. Click **Close**.

Note: These instructions were specific to Outlook XP. For instructions for other email clients, refer to your email client users guide for instructions on how to do this same activity.

The LDAP server is now setup, and users can search through the LDAP data directory for the names and email addresses of Lotus Foundations users.

Using Lotus Domino email clients

Lotus iNotes

When Lotus Foundations Start is installed, you can begin using iNotes to view and send email. In a Web browser that supports 128 bit encryption, go to the following URL:

```
http://server_ip_address/mail/
```

Enter a user ID and password that has been created in Lotus Foundations. Once you are authenticated, the iNotes screen is displayed.

For assistance with iNotes, use the help feature provided in iNotes.

Setting up Lotus Domino email clients

In addition to iNotes, you can install and use Windows client software to interact with Lotus Foundations Start email services. Lotus Notes is a client program designed specifically to take full advantage of features offered by a Lotus Domino server. Domino Access for Microsoft Outlook (DAMO) is an add-on for Microsoft Outlook clients that enables users to access email and calendar databases directly from a Domino server without using POP3 or IMAP. For Lotus Notes, see the *Lotus Foundations Start Getting Started Guide* section *Install the Lotus Notes add-on for Lotus Foundations Start* and for DAMO, see “Installing the Lotus Domino Access for Microsoft Outlook (DAMO) add-on.”

Installing the Lotus Domino Access for Microsoft Outlook (DAMO) add-on

One-click Lotus Foundations Start Domino for Microsoft Outlook (DAMO) installation

Lotus Domino Access for Microsoft Outlook is a method of accessing Domino-based email and collaboration materials through Microsoft Outlook. Using this client provides a user with full email, collaboration, and calendaring support, but it does not provide access to other Lotus Domino applications, such as team rooms and other business tools.

The one-click DAMO installation allows for users to install the DAMO plug-in onto their workstation in a single click. The administrator must first install an add-on module on IBM Lotus Foundations Start, which allows the DAMO settings to be automatically configured based on the Lotus Foundations Start server configurations.

Installing the IBM Lotus Foundations Start - DAMO feature to the server

To set up the one-click DAMO installation on the Lotus Foundations Start server:

1. If you have a DVD, insert the DVD labeled **Lotus Foundations Start Disk 2** into the server.
If you downloaded the software to your workstation, do the following:
 - a. Connect to the **autoinstall** file share on the Lotus Foundations server. To do this, from a workstation, click **Start** → **Run** and then enter ‘\’ followed by the server’s IP address, followed by \autoinstall. For example: \\192.168.0.1\autoinstall
 - b. Enter the administrative account and password.

- c. Locate the folder where you unzipped the Lotus Foundations Start DAMO package. The naming convention is lf-DAMO802-language_pack-nnnn.pkg (language groups G1, G2a, G2b); for example, lf-DAMO802-G1-2760.pkg.
 - d. Copy the DAMO file lf-DAMO802-language_pack-nnnn.pkg into the **autoinstall** folder. Wait to proceed until all of the files are copied to the server **autoinstall** folder.
2. At the WebConfig URL for the server (https://server_ip_address:8043), click **Software Update** from the menu on the left side of the WebConfig screen.
 3. A list of installable packages is displayed. If there is no list of available packages, wait several seconds and refresh the screen again. The DAMO add-on package should be listed and should be displayed as: Lotus Domino Access for Microsoft Outlook 8.0.2 for Gxx languages (Team autoinstall/lf-DAMO802-language_pack-nnnn.pkg).
 4. Click **Install** on the DAMO add-on; read and accept the license agreements. The installation begins immediately and might take a few moments.
 5. Verify the setup is complete on the main status page in the Add-ons section.

One-click installation and configuration of Lotus Domino Access for Microsoft Outlook to the workstation

Before installing Lotus Domino Access for Microsoft Outlook, ensure that all instances of Microsoft Outlook on the workstation are closed and that you are logged into the workstation using an account that has authorization to install software.

To install Lotus Domino Access for Microsoft Outlook, follow these steps:

1. From the user's workstation, connect to the user's file share on the Lotus Foundations server. To do this, click **Start** → **Run** and then enter '\\\' followed by the server's IP address, followed by \USERNAME. For example, type \\192.168.0.1\USERNAME where USERNAME corresponds to the user that you want to configure on the Lotus Foundations Server.
2. Navigate to **LotusFoundations** → **DAMO802_INSTALL** folder and double-click the DAMO_SETUP.BAT file, then select **Run** when prompted.

The DAMO Installation and Setup screen displays. Press any key to continue.

Note: When the command prompt window opens, a message is displayed that states: UNC paths are not supported. Defaulting to Windows directory. (as shown in the following screen shot). This message can be ignored.

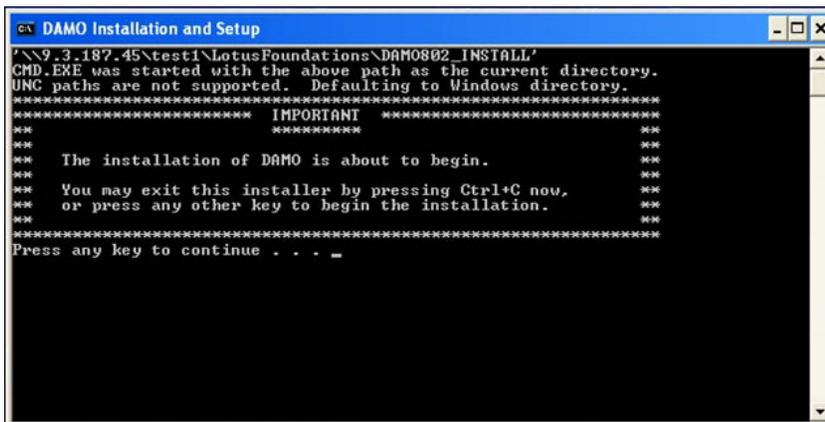


Figure 29. DAMO Installation and Setup screen

3. The installation should take approximately five minutes for a workstation that is on the same local network as the Lotus Foundations server. When the installation has completed, a message stating that "DAMO setup for USERNAME completed." Press any key to continue. The program closes.

4. Open Microsoft Outlook from either a desktop icon or the **Start** menu.
5. The first time you open Microsoft Outlook after running the DAMO setup, you are greeted with a Choose Profile window. Select the appropriate profile and click **OK**.
6. Enter the Lotus Domino password and click **OK**.
7. DAMO performs an initial setup that can take several minutes. When the initial setup is complete, Microsoft Outlook opens and the DAMO installation is complete. Microsoft Outlook then closes to finish initial replication upon the first time opening it with DAMO.

Web services

Web server

The high-performance Web server featured in Lotus Foundations is based on the industry standard Apache Web server and it supports Common Gateway Interface (CGI) scripts. Perl and PHP: Hypertext Preprocessor (PHP) are also integral parts of the Web services of Lotus Foundations.

Lotus Foundations provides Web services on a master Web server and on virtual Web servers.

Master Web server

What is the master Web server?

The master Web server is designed to serve your intranet site and the personal Web pages of your Lotus Foundations users. Although it is possible to make these sites available to outside users, you can choose to keep them private for security reasons.

Master Web services are provided from IP addresses assigned to the internal and external network interfaces of Lotus Foundations. If the Web server is enabled and access is granted to outside users, anyone accessing the Lotus Foundations server's internal or external Internet Protocol (IP) address from a Web browser can access information on the master server.

Webmaster directory

A webmaster team is created and configured as the master Web server administrator. When the webmaster team is created, a shared network directory called webmaster is made available to all members of the webmaster team, and the subdirectory WWW is created in the webmaster network drive. This is the directory from which intranet files are served. Any files saved in this directory are automatically accessible through the master Web site.

The webmaster directory also contains the log subdirectory, where server access and error logs are maintained, as well as a cgi-bin directory, where all Common Gateway Interface (CGI) scripts are stored.

Configuring your master Web server

To configure your master Web server, perform these steps:

1. Click **Web Server** in the left side menu of WebConfig. The **Basic Setup** tab of the Web Server Setup screen is displayed.

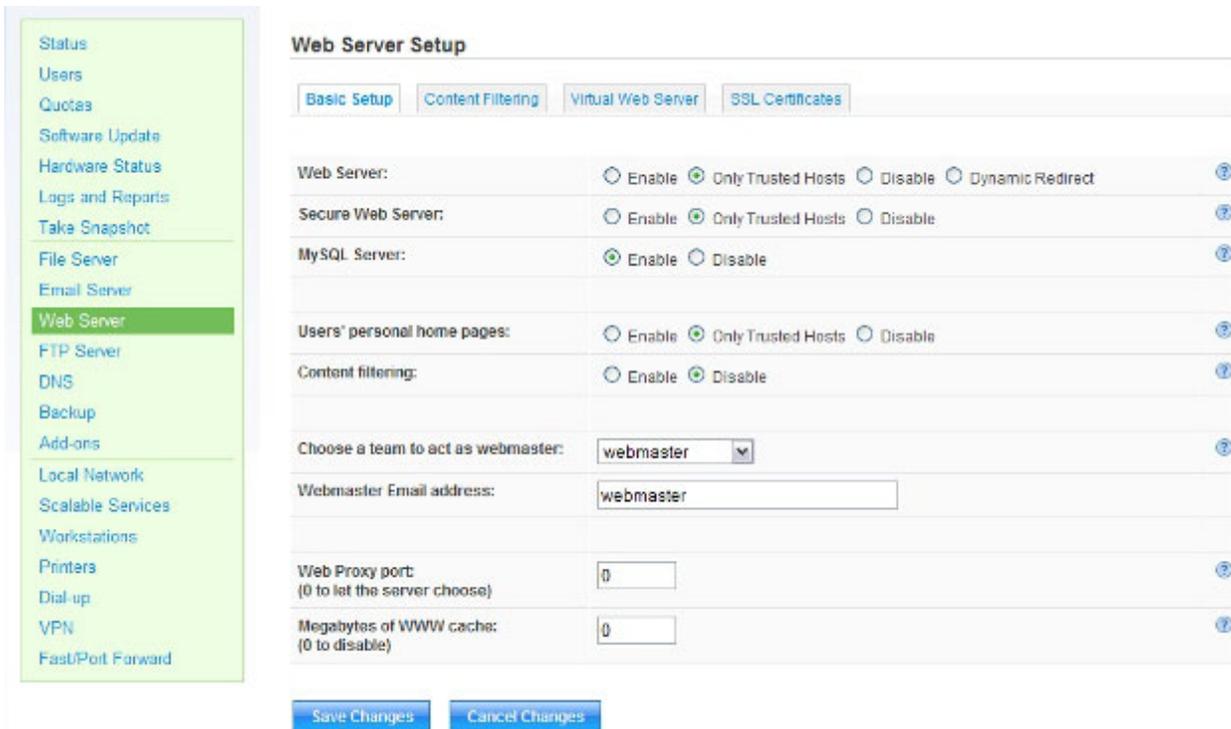


Figure 30. Basic Setup tab of the Web Server Setup page in the WebConfig console

2. In the **Web Server** field, select one of the following: **Enable**, **Only Trusted Hosts**, **Disable**, or **Dynamic Redirect**.

Table 10. Web Server enablement options

| Option | Description |
|--------------------|---|
| Enable | <ul style="list-style-type: none"> • Enables the Web server • Enables users on the internal network and users on the Internet to access Web pages on this server • Serves pages out of the webmaster's WWW directory • Web server logs are written in the webmaster's directory |
| Only Trusted Hosts | <ul style="list-style-type: none"> • Enables the Web server • Enables users on the internal network to access Web pages on this server • Serves pages out of the webmaster's WWW directory • Web server logs are written in the webmaster's directory |
| Disable | Disables the Web server; no one can access Web pages on this server |
| Dynamic Redirect | <ul style="list-style-type: none"> • Enables redirection of Web connections • Can be employed to circumvent blocked HTTP (Web) ports • All Web requests directed at Lotus Foundations are handled by a dynamic DNS server, automatically redirecting them to a different port on the Lotus Foundations server; redirection is almost transparent to clients, who may notice the host name and port changed slightly • DynamicDNS must be enabled (see the "Domain Name Service" on page 101 chapter for more information) |

3. In the **Secure Web Server** field, select one of the following: **Enable**, **Only Trusted Hosts**, or **Disable**.

Table 11. Secure Web Server enablement options

| Option | Description |
|--------------------|--|
| Enable | <ul style="list-style-type: none"> • Enables the secure Web server • Enables users on the internal network and users on the Internet to access Web pages on this server • Serves pages out of the webmaster's WWW directory • Web server logs are written in the webmaster's directory |
| Only Trusted Hosts | <ul style="list-style-type: none"> • Enables the secure Web server • Enables users on the internal network to access Web pages on this server • Serves pages out of the webmaster's WWW directory • Web server logs are written in the webmaster's directory |
| Disable | Disables the secure Web server; no one can access secure Web pages on this server |

4. In the **MySQL Server** field, select one of the following: **Enable** or **Disable**.

Table 12. MySQL Server enablement options

| Option | Description |
|---------|---|
| Enable | <ul style="list-style-type: none"> • Enables the MySQL server • Users on the internal network have access to personal databases and databases of any teams to which they belong |
| Disable | <ul style="list-style-type: none"> • Disables the MySQL server • Users do not have access to personal or team databases • Default setting |

User and team databases are automatically created when user and team accounts are set up. MySQL databases can be used to store dynamic Web page data for services such as online catalogs and stores.

MySQL is an advanced feature for users that are familiar with SQL (Structured Query Language). Refer to the "MySQL server" on page 127 chapter for more information.

5. In the **Users' personal home pages** field, select one of the following: **Enable**, **Only Trusted Hosts**, or **Disable**.

Table 13. Users' personal home pages enablement options

| Option | Description |
|--------------------|---|
| Enable | <ul style="list-style-type: none"> • Enables users' personal home pages to be viewed from anywhere • Master Web server must also be enabled • Format for addresses of personal home pages: <code>http://server.domain/~username</code> |
| Only Trusted Hosts | <ul style="list-style-type: none"> • Enables users' personal home pages to be viewed only from the local network • Master Web server must also be enabled • Format for addresses of personal home pages: <code>http://server.domain/~username</code> |
| Disable | Disables personal home pages |

This setting enables users to serve personal home pages to users on your network or the entire Internet from the WWW subdirectory located in each user's personal network directory.

6. In the **Choose a team to act as webmaster** field, select a team from the drop-down list to maintain the server. Although the webmaster team is created as the administrator of the master Web server and is listed as the default option for this field, any team can perform server maintenance tasks.

7. In the **Webmaster Email address** field, enter the e-mail address of the webmaster (the person in charge of the Web site), or a name of a user on the server.
8. In the **Web Proxy port** field, enter the appropriate Web proxy port. Leaving the default value of 0 enables the server to choose the Web proxy port.
9. In the **Megabytes of WWW cache** field, enter the appropriate number of megabytes for the WWW cache field. Refer to *“Web caching” on page 80* for more details.
10. Click **Save Changes**.

Virtual Web servers

Although virtual Web servers enable you to host a number of Web sites from the same server, these sites are displayed to outside users as though they are all hosted by different servers. To configure virtual Web servers on the outside interface, your Internet service provider (ISP) has to assign you multiple Internet Protocol (IP) addresses or you have to use name-based virtual Web sites, which use unique domain names to distinguish among Websites that share a single IP address.

Every virtual Web site must be associated with a maintenance team, which can maintain the content for only one virtual Web site. This content, though, can reside on different virtual Web servers. For example, you create a virtual Web server for `example.com` and one for `example.net`, but you want both sites to display the same information. You must create two virtual Web servers, but the virtual Web servers can share the same maintenance team. In contrast, if you want to display different content on `example.com` than what is displayed on `example.net`, the two virtual Web servers need two different maintenance teams.

If the virtual Web site is maintained by users on the local network, they can be made members of the maintenance team. If the site is maintained by outside users, they have to use File Transfer Protocol (FTP) to access to the Web site directory. If they have an account on the server, they can use their own login name and password. If they do not have an account on the network, they have to use the team name and password.

Creating a new virtual Web server

To create a new virtual Web server, perform these steps:

1. Click **Web Server** in the left-side menu of WebConfig. The **Basic Setup** tab of the Web Server Setup screen is displayed.
2. Click the **Virtual Web Server** tab.

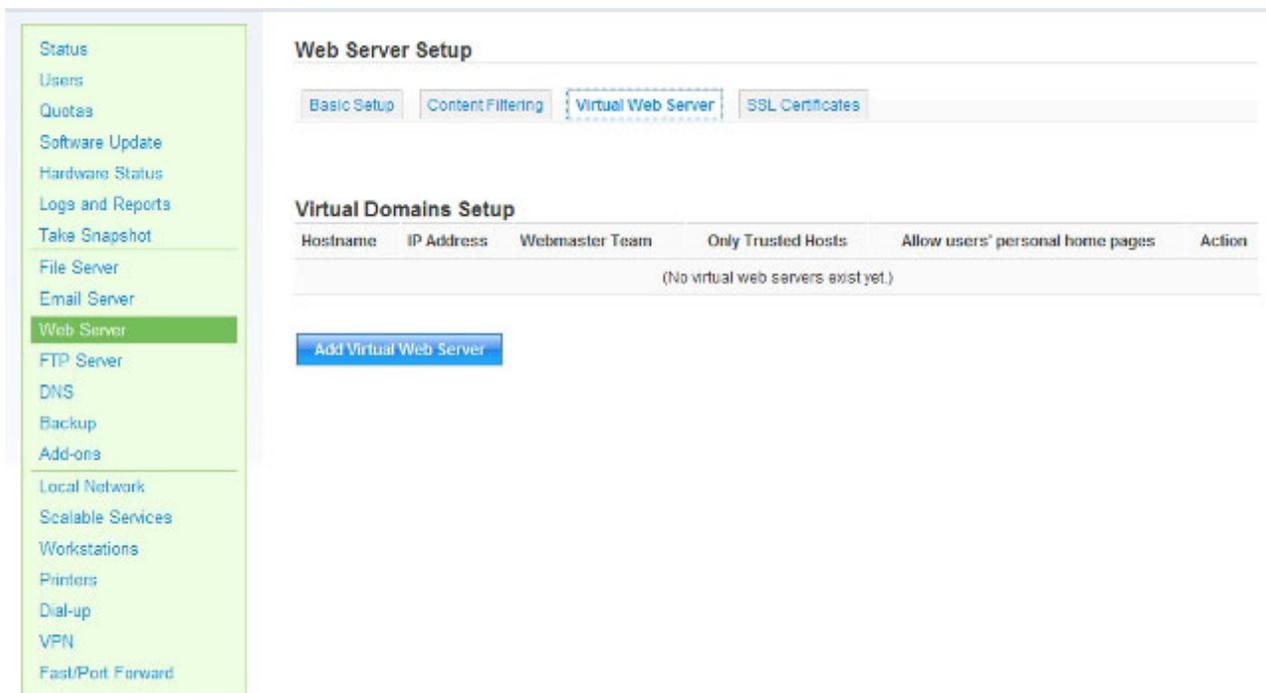


Figure 31. Virtual Web Server tab of the Web Server Setup page of WebConfig

3. Click **Add Virtual Web Server**. The New Virtual Domain screen is displayed.
4. In the **Hostname of Virtual Web Server** field, enter your Internet domain name. This host name is used as a Domain Name Service (DNS) entry for domain name resolution.
5. The name of your Lotus Foundations server automatically populates the **IP Address of Virtual Web Server** field. If you want to use a different IP address, enter it in this field.

Note: Your ISP must provide you with an extra IP address if you are configuring a virtual Web server on an outside, untrusted interface.

6. In the **Choose a team to act as webmaster** field, select a team to perform webmaster duties from the drop-down list.
7. In the **Trusted hosts only** field, select **Yes** or **No**. This option determines whether or not the virtual Web site is accessible only by trusted hosts. This option enables you to host both an intranet and a public Web site from the same server.
8. In the **Enable users' personal home pages** field, select **Enable** or **Disable**. This option determines whether or not you want to serve personal home pages from the WWW subdirectory located in each user's personal network directory.
9. Click **Save Changes**.

Deleting a virtual Web server

To delete a virtual Web server, perform these steps:

1. Click **Web Server** in the left-side menu of WebConfig, then click the **Virtual Web Server** tab of the Web Server Setup page. The Virtual Domains Setup section is displayed, showing all existing virtual domains.
2. Click the appropriate server's delete icon  in the Action column.
3. Click **OK** to confirm the deletion in the pop-up window.

All Web files for that server reside in the team's directory and are not deleted unless the team maintaining the site is deleted.

Editing a virtual Web server

To edit a virtual Web server, perform these steps:

1. Click **Web Server** in the left-side menu of WebConfig, then click the **Virtual Web Server** tab of the Web Server Setup page. The Virtual Domains Setup section displays all existing virtual domains.

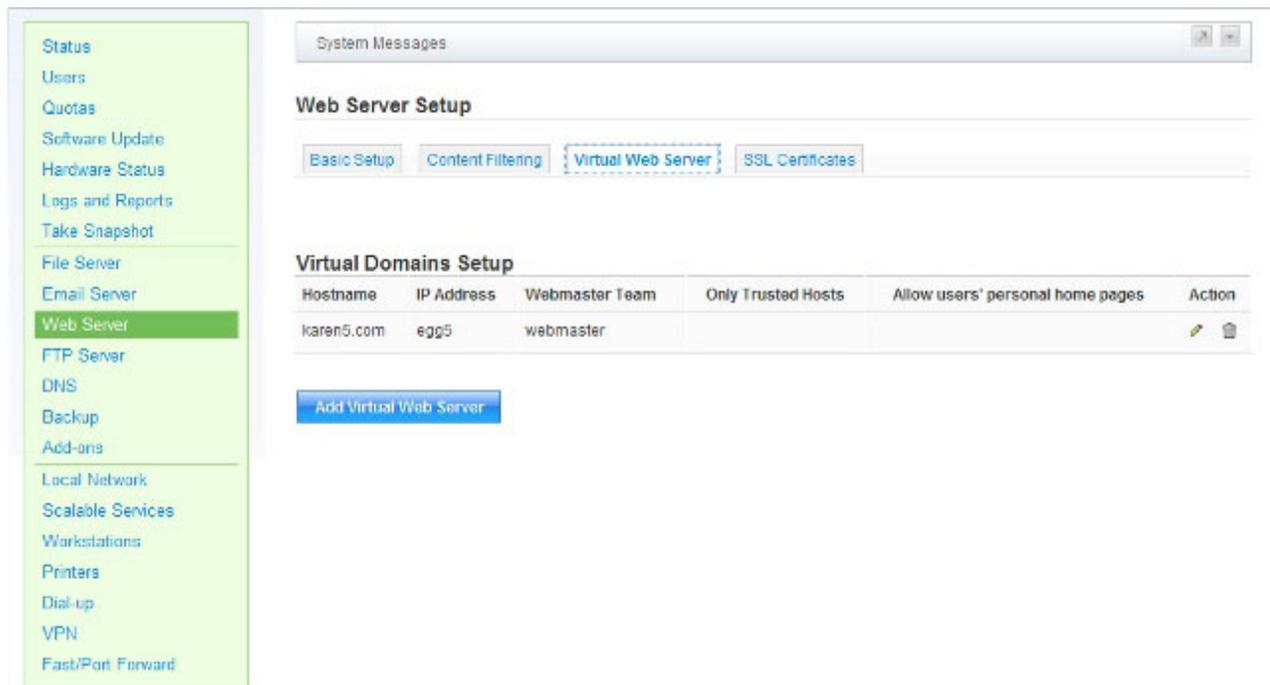


Figure 32. The Virtual Domains Setup section of the Web Server Setup page of WebConfig

2. Click the appropriate server's edit icon  in the Action column. The Modify Virtual Domain page is displayed.
3. Change the appropriate server settings.
4. Click **Save Changes**.

Hosting multiple Web sites

If your Lotus Foundations server is used as a Web hosting platform for a number of Web sites owned by various customers, you should use the following strategy.

For example, if your Lotus Foundations server is used to serve a Web site for AcmeWidgets, follow these steps:

1. Create a team called *AcmeWidgets*.
2. Create a virtual Web server and choose the *AcmeWidgets* team as the *Webmaster* team. Anyone from the *AcmeWidgets* team can access these files using File Transfer Protocol (FTP) with the username *AcmeWidgets* and the team's password.

Secure Web services

Secure Socket Layer (SSL) encryption

The Lotus Foundations Web server can serve secure Web pages, which are transmitted over the Internet using Secure Socket Layer (SSL) encryption technology. All browsers on the market support SSL encryption. For SSL to work, the Web server must have a file with a security certificate. This file is unique to every Web server and, for encryption to properly work, the certificate has to be issued by a proper certificate authority. When the user loads a secure page, its certificate is compared to the certificate held by the certificate authority. If they match, the site is considered trusted, and encrypted communication can commence.

You can purchase SSL security certificates from a number of Internet security companies.

Lotus Foundations security certificates

The security certificates that Lotus Foundations generates can be checked for authenticity by all Web browsers. The security certificate generated by Lotus Foundations is placed in the webmaster directory and named `certificate.pem`.

A user loading the first secure Web page from the server is warned that this security certificate is valid, but that the company issuing it cannot be considered trusted. The user has to manually approve the continuation of the transaction. Despite this warning, information exchanged between the Web browser and the Web server cannot be viewed by others.

If you purchase a security certificate from a certificate authority, delete the file automatically created by Lotus Foundations and replace it with the one you purchased. See the “*SSL certificate*” section in this chapter for more information. You might also want to store a copy of the purchased certificate in a different directory.

SSL certificate

Although a security certificate is automatically generated the first time you power up your Lotus Foundations server, you can overwrite this certificate at any time with a third-party certificate purchased from a certificate authority.

Note: You can only use X.509-based certificates.

Replace with a third-party certificate

To replace the automatically generated security certificate with a third-party security certificate, follow these steps:

1. Click **Web Server** in the left side menu of WebConfig. The **Basic Setup** tab of the Web Server Setup page is displayed.
2. Click the **SSL Certificates** tab.
3. Enter your personal information in the **PKCS#10 Request Specifics** fields.
4. Click **Generate PKCS#10 Request**. A Security Alert window is displayed. Click **Yes**.
5. The **System Message** box at the top of the page shows that Lotus Foundations is generating a new certificate request based on the information you provided in the previous steps. A new certificate request is generated in the **PKCS#10 Certificate Request** box.
6. Copy and paste the new certificate request from the **PKCS#10 Certificate Request** box and give it to your certificate authority. They use this to generate a new certificate.
7. Once you have received the new certificate from your certificate authority, copy and paste it into the X.509 Certificate box.
8. Click **Replace Certificate**.

Web caching

To improve bandwidth, Lotus Foundations can temporarily store Web files accessed by internal users in a cache. If a user requests any of these stored files, Lotus Foundations serves them from the cache instead of from the original Web site. Internet bandwidth is used only to retrieve Web pages that have not previously been viewed, resulting in much faster access to the Internet.

Configuring Web caching

To configure Web caching, perform these steps:

1. Click **Web Server** in the left side menu of WebConfig. The **Basic Setup** tab of the Web Server Setup page is displayed.
2. Enter the amount of data to be cached in the **Megabytes of WWW cache** field. Specify 5-10 MB for every active user on the internal network.
 - Once the cache is full, the oldest files are deleted to make space for new ones.
 - Configuring the cache size to zero disables the Web cache server.
3. Click **Save Changes**.
4. For Web caching to run transparently, ensure that your Web browser is not configured to use a proxy server.

Web filtering

Web and content filtering

Lotus Foundations provides positive Web filtering, which is a feature that enables the system administrator to permit access to specific Internet sites, while blocking access to all others.

Enabling the Web filter

Follow these steps to enable the Web filter:

1. Select **Web Server** from the left-side menu in WebConfig. The Web Server Setup screen is displayed.
2. In the **Content filtering** field, select **Enable**.
3. Click **Save Changes**.

If you plan to use Web filtering in conjunction with Web caching, all proxy server settings must be removed.

Providing full internet access

To provide a specific workstation with access to all Internet sites, follow these steps:

1. Click **Web Server** from the left-side menu in WebConfig.
2. Click the **Content Filtering** tab.
3. Enter their host name or IP address in the "Workstations Exempt from Filtering" section of the screen.
4. Click the green plus sign to add the entry. The new entry is displayed in the list of workstations with full access.

To remove full access for a workstation, click the delete action button located next to the workstation name or IP address. The exemption list can take up to two minutes to refresh.

Port exemptions

When enabled, the Lotus Foundations content filter monitors port 80 and all others above 1023 (1024-65535). If an application uses a port between 1024 and 65535 that you need to open, follow these steps to permit that application to bypass the content filter. Note that all other applications using this port also are exempt from Web filtering.

1. Click **Web Server** from the left-side menu in WebConfig.
2. Click the **Content Filtering** tab.
3. Enter the port number you want to exempt in the "Ports Exempt From Filtering" section.
4. Click the green plus sign to add the entry.

Adding permitted Websites

For users to access a specific Website, the administrator has to add it to the Permitted Websites list. By default, the Websites `lotus.com` and `ibm.com`[®] are automatically added.

To add a Website you want to permit all users access to, follow these steps:

1. Click **Web Server** from the left-side menu of WebConfig.
2. Click the **Content Filtering** tab.
3. In the Permitted Websites section, enter the site's name in the empty **Add New Website** field. To view the permitted Website list, click **Display Permitted Website List**.
4. Click the green plus sign to accept the change. The Website you entered is now displayed in the permitted Websites list.
 - You can use wildcards to enable all prefixes of a given domain. For example, to enable `www.example.com`, `my.home.example.com`, and `office.example.com`, type:
`*.example.com`
 - You can use wildcards in the place of any label (dot-separated block) within a domain name. To do this, replace any label of the domain with an asterisk. For example, in order to enable both `example.com` and `example.org`, type:
`example.*`
 - The two rules above cannot be used at the same time. For example, `*.example.*` permits `www.example.com`, `office.example.org`, but not `my.home.example.org`.

Adding denied Websites

To manually add a denied Website for the first time, follow these steps:

1. Click **Web Server** from the left-side menu of WebConfig.
2. Click the **Content Filtering** tab.
3. Go to the Denied Websites section. Enter the Website address in the **Add New Website** field.
4. Enter the reason for denial. This section is optional.
5. Click the green plus sign to add the entry. When this is done, the Denied Websites box displays a link labeled **Display Denied Website List**. You can either click this link to view the current list and add new entries or add new entries on the main.

Accepting access requests

If a user has requested access to a Website that has not been authorized, a notice is displayed in their browser.

The user can request that this site be authorized by the administrator by clicking the **Request Access** button.

The administrator can view the all the pending requests in the main Content Filtering section of WebConfig by clicking the link Display Pending List.

To accept or deny requests, follow these steps:

1. Click **Web Server** from the left-side menu of WebConfig.
2. Click the **Content Filtering** tab.
3. Click **Content Filtering Requests**.
4. A list containing the requested sites is displayed. Choose to permit the site by clicking the green plus icon.

Users can now access the permitted Website.

Denying access requests

To deny a requested Website, follow these steps:

1. Click **Web Server** from the left-side menu of WebConfig.
2. Click the **Content Filtering** tab.
3. Click **Content Filtering Requests** as you would if you were going to accept a request. The list of pending requests is displayed.
4. If you want to immediately deny the request, click the delete button. If you want to provide a reason, click the edit action button and enter it into the field labeled **Reason for Denial**. When you are done, click **Deny Request**.

List management

The list management feature enables you to import and customize content filtering lists from other Lotus Foundations servers. You can export and customize the local content filtering list to share with other Lotus Foundations servers.

Importing a list

To import a content filtering list you must first obtain an exported list from another Lotus Foundations server. Refer to "Exporting a list" for how to do this. After this is done, follow these steps:

1. Click **Web Server** from the left-side menu of WebConfig.
2. Click the **Content Filtering** tab.
3. Click **Import/Export Website Lists**
4. Choose whether or not you want the imported list to include the list of permitted websites. Click either the **Enable** or **Disable** radio button.
5. Choose whether or not you want the imported list to include the list of denied Web sites. Click either the **Enable** or **Disable** radio button.
6. Click the **Browse** button in the **File To Import** field and locate the file you want to import. The file name and path should now be displayed.
7. Click **Import Lists**.

Exporting a list

To export a content filtering list, follow these steps:

1. Click **Web Server** from the left-side menu of WebConfig.
2. Click the **Content Filtering** tab.
3. Click **Import/Export Website Lists**
4. Choose whether or not you want the exported list to include the list of permitted Websites. Click either the **Enable** or **Disable** radio button.

5. Choose whether or not you want the exported list to include the list of denied Websites. Click either the **Enable** or **Disable** radio button.
6. Click **Export Lists**. A text file is generated that you can save and use to port to another Lotus Foundations server.

Email reporting

The Lotus Foundations content filter can send instant email notifications every time a website has been requested and email a daily report of all requested sites.

To use the email reporting options, follow these steps:

1. Click **Web Server** from the left-side menu of WebConfig.
2. Click the **Content Filtering** tab.
3. Click **Configure Report Options**. The Content Filter Reporting Options screen is displayed.
4. To enable daily reports, set the **Daily Reports** to **Enabled**. That this feature requires the internal SMTP server to be enabled.
5. If you enabled daily reports, in the **Time of Day for Daily Report** drop-down, choose the time of day that the daily report of pending content filtering requests is to be mailed to the administrator. 0:00 represents midnight.
6. To enable instant notification, set **Instant Notification** to **Enabled**. This feature requires the internal SMTP server to be enabled.
7. Enter the email address for the administrator in the **Administrator's Email Address** field.
8. Click **Save Changes**.

FTP services

FTP Server

Lotus Foundations uses a File Transfer Protocol (FTP) server that enables users and teams to access network and Web files. FTP services are automatically enabled for users on the internal network.

Anonymous FTP Server

The FTP server can be used in anonymous mode to enable uploads and downloads of files to a specific directory without authentication from the remote user. This anonymous mode of operation is commonly used for public file distribution on the internet. Although the file can be downloaded from a Web server, FTP is the preferred method because it offers superior performance for high volume and large file transfers.

When **Anonymous FTP** is enabled, Lotus Foundations automatically creates a team called FTP. Members of this team have access to the FTP directory. All files placed in this directory by team members are accessible to anyone on the Internet. Similarly, when **Anonymous Upload** is enabled, anyone on the Internet can upload their own files to the subdirectory in the FTP directory.

Enabling the FTP server

1. Click **FTP Server** in the left-side menu of WebConfig. The FTP Server Setup screen is displayed.

FTP Server Setup

| | |
|--------------------------------|--|
| FTP file server: | <input type="radio"/> Enable <input checked="" type="radio"/> Only Trusted Hosts <input type="radio"/> Disable |
| Anonymous FTP: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Anonymous uploads: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| Maximum number of connections: | <input type="text" value="100"/> |

Save Changes

Cancel Changes

Figure 33. FTP Server Setup screen

2. Indicate whether or not you want to enable the FTP file server.
3. Indicate whether or not you want to enable anonymous FTP.
 - If this option is enabled, anyone can download files from the FTP directory by using anonymous as the FTP login name and their email address as the password.
4. Indicate whether or not you want to enable anonymous uploads.
 - If this option is enabled, anonymous users can upload files to the FTP directory. Be careful with this option.
5. Enter the total number of connections at any one time.
 - This option is used to prevent the overuse of internet bandwidth. You can leave the default setting, but increase the number of anonymous users if the server is often busy.
6. Click **Save Changes**.

Enabling FTP access for a specific team or user

Follow these steps to enable FTP access for a specific team or user:

1. Select **Users** from the left-side menu of WebConfig.
2. Click the appropriate user or team's edit icon .
3. The Modify Users or Modify Teams screen is displayed.
4. Indicate whether or not you want this user or team to have FTP access in the **Allow FTP Access** field.
5. Click **Save Changes**.
6. Repeat steps 2-5 for any additional users or teams.

User vs. Team FTP access

Users can log into the Lotus Foundations FTP server by entering their assigned username and password to access their own user directory.

To access the directory of any team of which they are a member, users need to use the team name in place of their user names, but they can continue to use their individual passwords rather than a team password.

Software update

Periodically, Lotus Foundations contacts distribution servers through its internet connection and requests an updated list of available software releases. A list of available software releases is found on the Software Update screen.

Upgrading Lotus Foundations

Note: If you are running Lotus Foundations from a CD or DVD, you must configure your disks from the WebConfig menu, shut down the system, remove the Lotus Foundations CD and restart the system before Software Update can work. For more information on configuring the hard disks, see “Disk management” on page 110.

It is best to upgrade the software after-hours because rebooting disconnects all users and causes all services to stop functioning until the server has restarted.

1. Select **Software Update** from the left-side of WebConfig. The Software Update screen is displayed, showing the Lotus Foundations software version the server is currently running and all versions available for download.

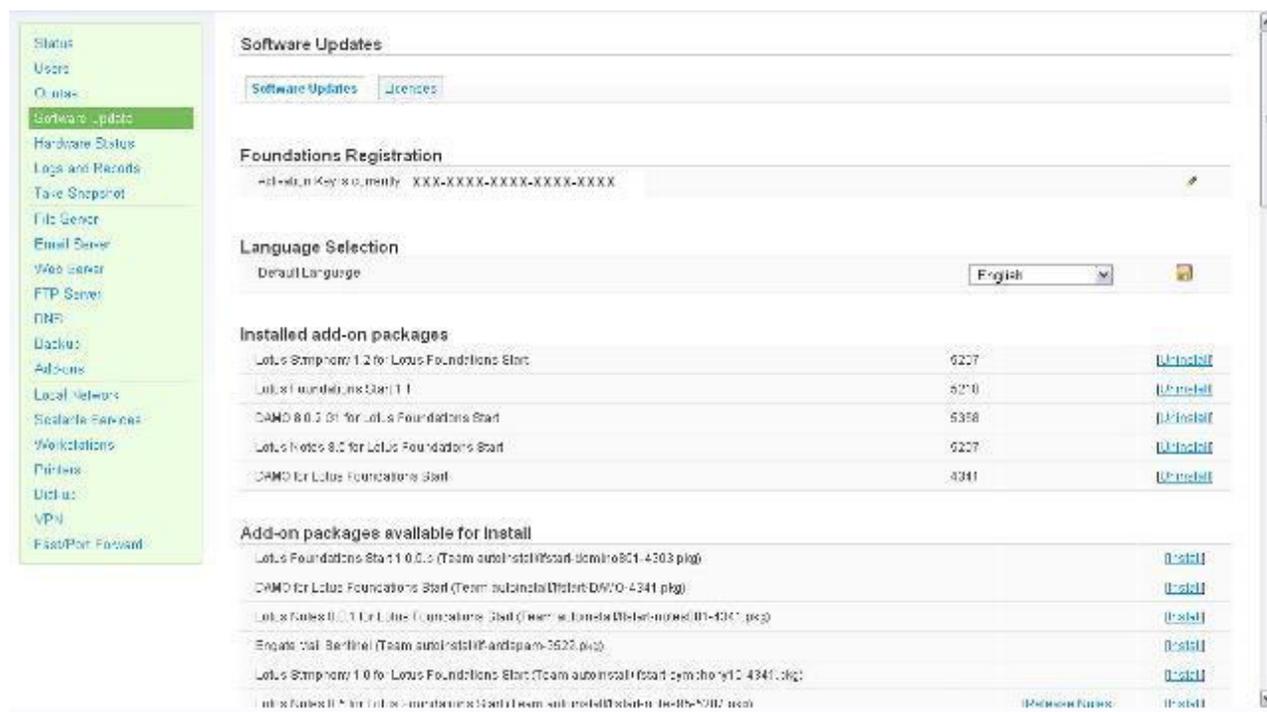


Figure 34. Software Update screen

2. Scroll to the bottom of the screen and click **Check for New Versions** to update the list of available versions.
The System Status screen is displayed. The Software Update line displays the progress.
3. Click on a version's **Release Notes**® link to access its release notes.
 - The release notes outline the version's new features and provide important information that you need to know before upgrading your software. Read the release notes carefully.
4. The new software has to be downloaded to the server. To do so, click the appropriate version's **Download** link. Read and accept the licenses. The System Status screen is displayed. The Software Update line displays the progress of the download.

5. When the download is complete, the Software Update line tells you that a software update has been installed and prompts you to reboot your system.
6. Click the **Reboot** link.
7. Click **Return** when an IP address is displayed on the Lotus Foundations server's display console. The System Status screen is displayed. The Software Update line asks if you want to keep the new software release:
 - Selecting **Yes** permanently installs the new operating system.
 - Selecting **No** reboots the Lotus Foundations server and reverts to the previous operating system.
8. If Lotus Foundations is not installed properly, the server uses the old version when it reboots. If the server encounters any difficulty starting the new operating system, the previous version starts instead. If you choose not to confirm your download, and a power loss or reboot occurs, the server reverts back to the last-used operating system.
9. To revert back to the old version, select **Software Update** from the WebConfig menu. Click the **Activate** link in the "Foundations Versions already installed" section of the screen:

Switching languages

Lotus Foundations currently enables you to view WebConfig in various different languages. To switch between languages, follow these steps:

1. Click **Software Update** from the left-side menu of WebConfig.
2. In the **Software Updates** tab, locate the section titled **Language Selection**.
3. Using the drop-down box, select the target language.
4. Click the save icon to save the change.

To add language packs or change the language for the Lotus Domino server and the Lotus Notes client, see the *Lotus Foundations Start Getting Started Guide*.

Virtual private networks

Private networks

In the past, private networks were created by using routers to connect different office locations through dedicated lines. This procedure is often called a wide area network (WAN). Conventional private networks are illustrated like this:

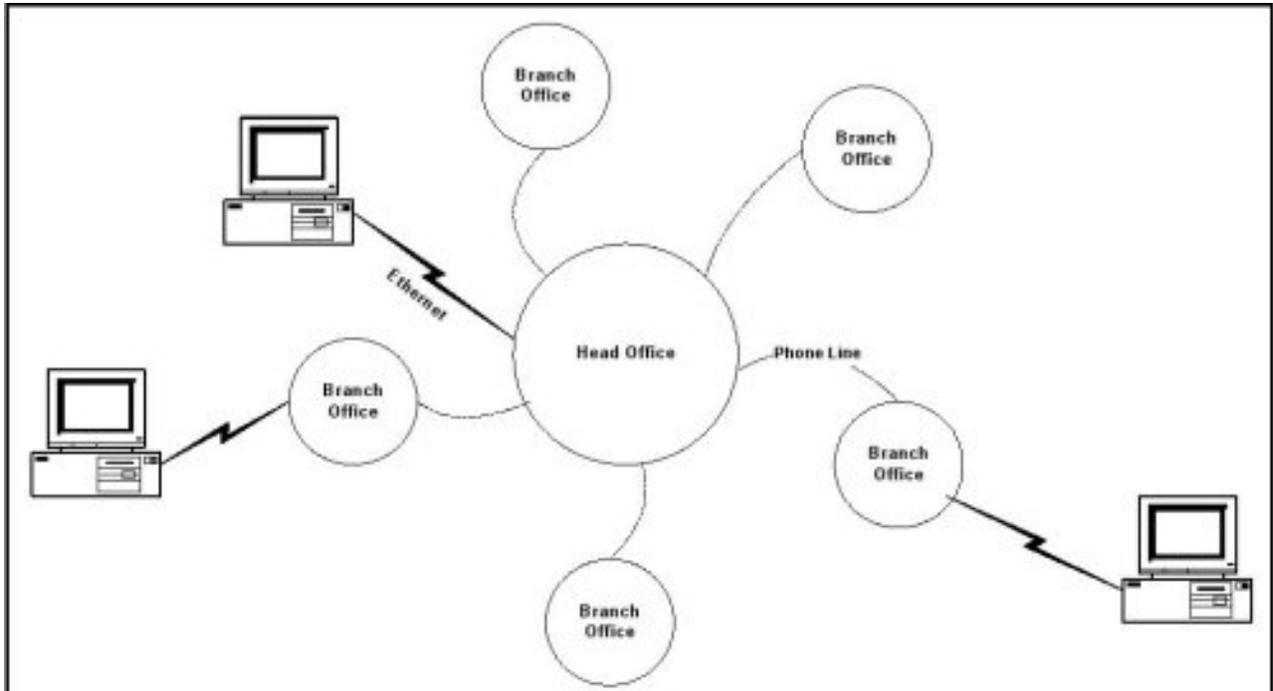


Figure 35. WAN private network

Virtual private networks

TunnelVision enables you to create a virtual private network (VPN) using the internet instead of a dedicated WAN connection for server-to-server or network-to-network connections. A VPN is illustrated as in the following diagram:

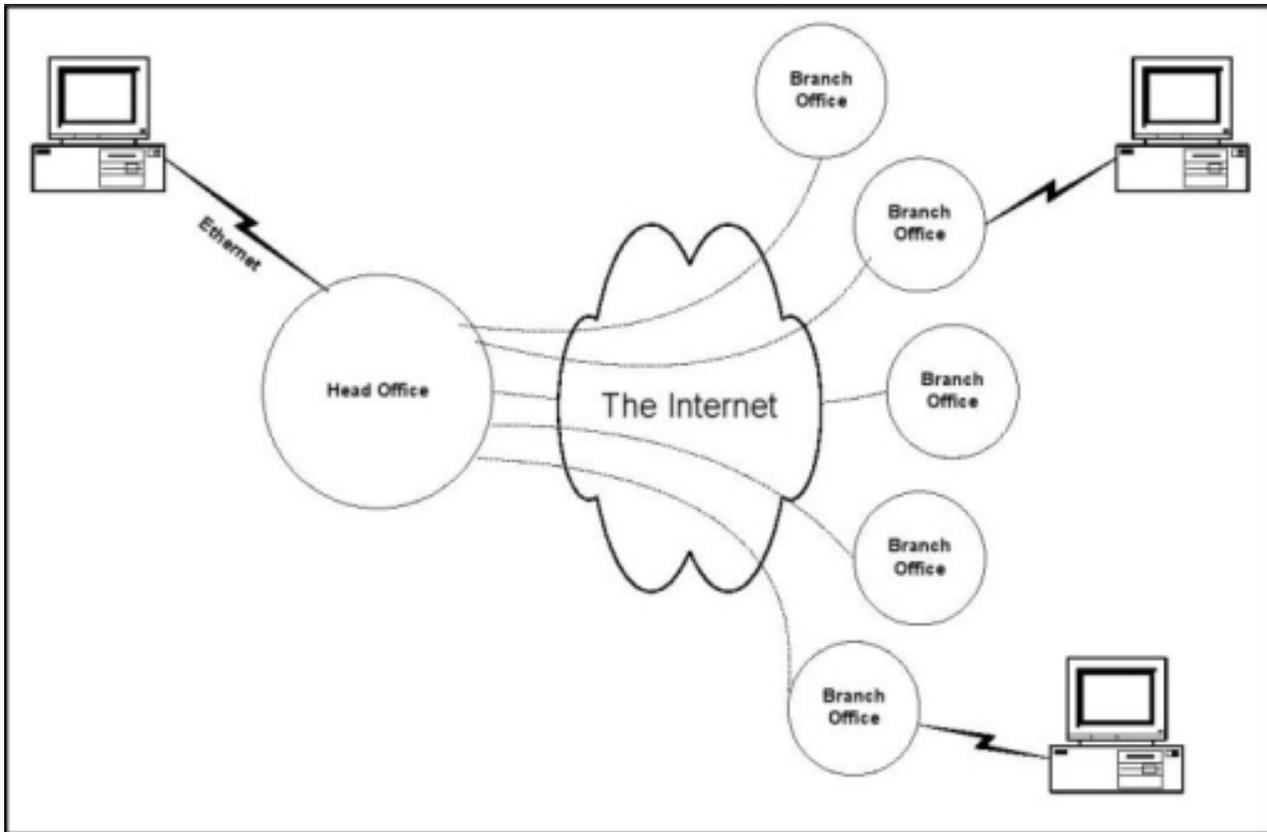


Figure 36. VPN topology

For remote and mobile employees, see “Remote access services” on page 95 for instructions on setting up client connections using VPN.

Making a virtual network private

In a conventional private network, the company owns all the routers, all the computers, and all the phone lines involved. Because the only people using the network are employees, the network is secure, at least in theory.

The internet, on the other hand, is connected to any number of businesses and organizations. As private data passes through the internet, it is possible that people might intercept what is being sent. To prevent this from happening, all of the data that passes through a VPN is encrypted with the strongest encryption technology available: 1024-bit RSA and 128-bit Blowfish algorithms. Such encryption makes it difficult to access the data in your transmissions.

VPN network topologies

Topology refers to the shape of a network or the network’s layout. How different nodes in a network are connected to each other and how they communicate are determined by the network’s topology. A VPN enables organizations to interconnect their offices securely. Applications and data can be readily shared throughout the VPN network if desired. For example, you could have the accounts departments of each branch connected to each other or each department could be connected to a central point.

TunnelVision can work in either a ‘fully-meshed’ topology or a ‘non-meshed’ topology.

Fully-meshed topology

In a fully-meshed topology, devices are connected with many redundant interconnections between network nodes. In a true meshed topology, every node has a connection to every other node in the network. An advantage of such a network would be that no branch is reliant upon a single connection.

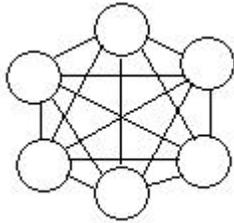


Figure 37. Diagram of a fully-meshed topology

Non-Meshed Topology

In a non-meshed or 'hub-and-spoke' topology all devices are connected to a central hub or headquarters that dictates the access rules of the VPN to the other branches. Nodes communicate across the network by passing data through the hub. A typical application would be to implement a terminal services solution using the headquarters as the gateway for the branch sites.

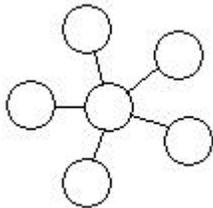


Figure 38. Diagram of a non-meshed topology

How TunnelVision works

A VPN enables all of the computers on two networks to communicate with each other. For this to happen, you have to first configure their subnet addresses.

When you install Lotus Foundations, the IP addresses used on the local network do not really matter. Internet standards recommend that all IP addresses that are owned by internal business networks (and not used on the internet itself) begin with 192.168. The third part of the IP address specifies which private subnet number you are using, and the fourth part identifies an individual computer on the network. In special circumstances, however, you can use any subnet number at all (the first three parts of the IP address). Non-routable IP networks can be any of the following:

- 10.0.0.0 - 10.255.255.255
- 172.16.0.0 - 172.31.255.255
- 192.168.0.0 - 192.168.255.255

The important thing is that the Lotus Foundations server and the computers on the local network have the same subnet number and unique IP addresses.

Network address translation (NAT)

When you communicate with other computers on the internet, Lotus Foundations uses network address translation (NAT) to give each connection a valid, unique IP address that does not conflict with other networks.

But for a VPN, Lotus Foundations should not use NAT because then only two addresses are visible: Lotus Foundations server #1 and Lotus Foundations server #2. Instead, Lotus Foundations should pass addresses on each network through to the other network unchanged.

For this to happen, you need to assign different subnet numbers to each Ethernet network involved in the VPN. For example, use 192.168.1 for Network #1 and 192.168.2 for Network #2. That means each computer on Network #1 has an address starting with 192.168.1, and each computer on Network #2 has an address starting with 192.168.2.

The steel pipe (or tunnel)

Network #1 is connected to the internet through Lotus Foundations server #1 and has the subnet number 192.168.1. Network #2 is connected to the internet through Lotus Foundations server #2 and has the subnet number 192.168.2.

Gateway settings work when a computer on the Ethernet sends packets directly to another computer if its subnet number is the same. That means that 192.168.1.15 transmits directly to 192.168.1.46, since they are both on the same subnet. However, 192.168.1.15 cannot send packets directly to 192.168.2.20 - the subnet numbers are similar, but they are not the same. The station then sends the data through its default gateway: Lotus Foundations server #1.

This is where TunnelVision is used, as long as you have configured the Lotus Foundations servers to create a VPN. When TunnelVision starts, it creates an encrypted connection between the two Lotus Foundations servers through the Internet. This connection is sometimes called a steel pipe because, like a true steel pipe, it is hard to see what is inside or to break through it. More often it is known as a tunnel.

Lotus Foundations server #1 treats data addressed to Network #2 from its local Ethernet in a special way. Rather than just passing the data to the ISP, Lotus Foundations encrypts it and sends it through the tunnel. When Lotus Foundations server #2 receives the encrypted data, it decrypts the information and forwards it on to Network #2 as if it had arrived directly from Network #1. That way, Network #1 can communicate securely with Network #2 without any need for special changes to individual workstations.

Creating a VPN (server-to-server)

Because the Lotus Foundations server does most of the work for you, creating a VPN is much easier than it sounds. All you have to do is create the encrypted tunnel.

Using unique subnet numbers

Each Ethernet network in the VPN must use a different subnet number. Use any of the networks from 192.168.1 to 192.168.254, since these numbers are specifically reserved for private use. As noted in "How TunnelVision works" on page 89, there are three available address ranges for non-routable IP networks.

The master server needs an IP address or FQDN

The only way to find someone on the internet is to know their IP address. This can be accomplished with either a static IP address (a static IP address is guaranteed never to change so people on the Internet can always find you) or through the use of a fully qualified domain name (FQDN) such as server.domain.com. The DNS system translates the FQDN into an IP address. This is particularly useful for systems that utilize dynamic DNS.

The Lotus Foundations Dynamic Domain Name System (DDNS) feature automatically updates DNS information when a new IP address is assigned to a network, enabling you to publish DNS entries and provide internet services even if you have a dynamic IP address.

To create a connection between two Lotus Foundations servers, someone needs to act as the client and someone as the master server. It is similar to a phone call to an ISP: you, the client, need to know their phone number, but they, the server, do not need to know yours. With TunnelVision, you have a similar situation: the server side, accepting a connection, needs a static IP address or FQDN, while the client side can have either a static or dynamic IP address.

Only one Lotus Foundations server, usually the computer with the fastest internet connection at the head office, needs to act as the server and have a static IP address or fully-qualified domain name. All the others can simply act as clients.

To obtain a static IP address, talk to the ISP. Dynamic DNS can be used in place of a static IP address. Refer to “Domain Name Service” on page 101 for more information.

Configuring a TunnelVision master server

Ensure that the Lotus Foundations server that you are configuring as the Master server has a static IP address or has a fully-qualified domain name.

1. Select **VPN** from the left-side menu in WebConfig. The VPN Setup screen is displayed.

| VPN Setup | |
|--|---|
| VPN Setup | IPsec Setup |
| PPTP Server: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| TunnelVision: | <input type="radio"/> Enable <input checked="" type="radio"/> Disable |
| TunnelVision: Use Fully Meshed Mode: | <input checked="" type="radio"/> Yes <input type="radio"/> No |
| TunnelVision: Address of Master Server: | <input type="text"/> |
| TunnelVision Password: | <input type="password"/> |
| Re-enter TunnelVision Password: | <input type="password"/> |
| Save Changes | Cancel Changes |

Figure 39. VPN Setup screen

2. Select **Enable** for the **PPTP Server** setting.
3. Select **Enable** for the **TunnelVision** setting.
4. Select **Yes** for the **TunnelVision: Use Fully Meshed Mode** setting to run TunnelVision in a Fully Meshed mode and **No** to run it in a non-meshed mode.

- If you enable TunnelVision to work in fully-meshed mode, then your server can learn about other servers on the VPN by exchanging information through the master server. Then each server makes connections directly to each of the other VPN-connected servers directly, as needed, without needing to go through the master. If you disable fully-meshed mode, then your server only communicates directly with the master server and the master's local network. Your server cannot see any of the other VPN-connected servers or networks.
 - In previous versions of the Lotus Foundations software, fully-meshed mode was always enabled and this is still the recommended setting.
5. Leave the **TunnelVision: Address of Master Server** field empty since the master server does not initiate connections.
 6. Enter a password that the server and client use to prove to each other that they are trusted.
 7. Re-enter the password to ensure it was entered correctly.
 8. Click **Save Changes**.

Configuring a TunnelVision client

A Lotus Foundations server does not need a static IP address to act as a TunnelVision client, but it needs to know the static IP address or fully-qualified domain name of the master server.

To find this information, select **Local Network** from the left-side menu in the WebConfig console on the master server. Click **Advanced Setup** tab. Note the address assigned to eth1.

1. Select **VPN** from the left-side menu in WebConfig. The VPN Setup screen is displayed.
2. Leave the default PPTP Server setting.
3. Select **Enable** for the **TunnelVision** setting.
4. Select **Yes** for the **TunnelVision: Use Fully Meshed Mode** setting if you are running TunnelVision in a fully-meshed mode, and **No** if you are running it in a non-meshed mode.
 - If you enable TunnelVision to work in fully-meshed mode, then your server can learn about other servers on the VPN by exchanging information through the master server. Then each server makes connections directly to each of the other VPN-connected servers directly, as needed, without needing to go through the master. If you disable fully-meshed mode, then your server only communicates directly with the master server and the master's local network. Your server cannot see any of the other VPN-connected servers or networks.
 - In previous versions of the Lotus Foundations software, fully-meshed mode was always enabled and this is still the recommended setting.
5. In the **TunnelVision: Address of the Master Server** field, enter the master server's static IP address or fully-qualified domain name.
6. Enter the password that was used in step 6 of "Configuring a TunnelVision master server" on page 91.
7. Re-enter the password to ensure it was entered correctly.
8. Click **Save Changes**.
 - TunnelVision immediately begins to create the tunnel between the client and the master server. If the client and the server are connected to the internet and everything is configured correctly, this process should only take a few seconds.

To configure another Lotus Foundations server as a client, simply repeat this process.

TunnelVision status

The System Status screen always displays the status of active VPNs. You might need to click the browser's **Refresh** button to see the latest information.

The idle time-out

If either end of the tunnel does not receive any data for approximately 20 minutes, it assumes that one end has disconnected from the Internet or that the tunnel is no longer needed.

If one end of the tunnel is still online, it tries to rebuild the connection automatically. Since this only takes a few seconds and happens only when the tunnel has been idle for a long time, this should not affect you. However, this behavior can often cause the VPN Tunnel's status light to turn yellow or red. This is not a sign of malfunction.

IPsec

Known configurations

The IPsec functionality in Lotus Foundations uses the industry standard ISAKMP/IKE protocol and is compatible with other standard IPsec devices.

Adding an IPsec route

To create a new IPsec route, follow these steps:

1. Select **VPN** from the left-side menu WebConfig.
2. Select the **IPsec Setup** tab.
3. Select **Add New IPsec Route**. The Create IPsec Route screen is displayed.

| Create IPsec Route | |
|--------------------------------|---|
| Remote Server: | <input type="text"/> |
| Remote Subnet: | <input type="text"/> |
| Local Subnet: | 9.3.187.0/25 |
| Remote IKE key: | <input type="text"/> |
| Perfect Forward Secrecy (PFS): | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Enable this connection: | <input checked="" type="radio"/> Yes <input type="radio"/> No |

Figure 40. Create IPsec Route screen

4. In the **Remote Server** field, enter the public IP address or the fully-qualified domain name (FQDN) of the remote server.
5. To include a private subnet behind the remote server's firewall, enter the internal subnet containing the internal IP address of the remote unit in the **Remote Subnet** field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, enter 192.168.10.0/24.
6. Enter a remote IKE key. This is a password that should be unique and entered on both ends of the IPsec connection.

7. Click **Yes** to enable the **Perfect Forward Secrecy (PFS)** feature. The two ends do not negotiate this automatically, so make sure that the setting is the same on both ends.
8. For **Enable this connection**, click **Yes**.
9. Click **Save Changes**.

Adding an anonymous incoming connection IPsec route

Creating an anonymous IPsec route eliminates the need for statically identifying the remote server IP address.

To configure an anonymous connection, follow these steps:

1. Select **VPN** from the left-side menu in WebConfig.
2. Select the **IPsec Setup** tab.
3. Select **Add New IPsec Route**. The Create IPsec Route screen is displayed.

Create IPsec Route

| | |
|---------------------------------------|---|
| Remote Server: | <input type="text"/> |
| Remote Subnet: | <input type="text"/> |
| Local Subnet: | 9.3.187.0/25 |
| Remote IKE key: | <input type="text"/> |
| Perfect Forward Secrecy (PFS): | <input type="radio"/> Yes <input checked="" type="radio"/> No |
| Enable this connection: | <input checked="" type="radio"/> Yes <input type="radio"/> No |

Figure 41. Create IPsec Route screen

4. Enter 0.0.0.0 in the **Remote Server** field. The Lotus Foundations server must have a static IP address.
5. To include a private subnet behind the remote server's firewall, enter the internal subnet containing the internal IP address of the remote unit in the **Remote Subnet** field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, enter 192.168.10.0/24.
6. Enter a remote IKE key. This is a password that should be unique and entered on both ends of the IPsec connection.
7. Click **Yes** to enable the **Perfect Forward Secrecy (PFS)** feature. The two ends do not negotiate this automatically, so make sure that the setting is the same on both ends.
8. For **Enable this connection**, click **Yes**.
9. Click **Save Changes**.

Editing an IPsec route

To edit an existing IPsec route, follow these steps:

1. Select **VPN** from the left-side menu in WebConfig.
2. Select the **IPsec Setup** tab.

3. Select the appropriate IPsec route's edit icon  on the IPsec Setup screen.
4. The Modify IPsec Route screen is displayed.
5. In the **Remote Server** field, enter the fully-qualified domain name or IP address of the remote server that you want to connect to.
6. To include a private subnet behind the remote server's firewall, enter the internal subnet containing the internal IP address of the remote unit in the **Remote Subnet** field. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, enter 192.168.10.0/24.
7. Enter a remote IKE key. This is a password that should be unique and entered on both ends of the IPsec connection.
8. Select **Yes** to enable the **Perfect Forward Secrecy (PFS)** feature. The two ends do not negotiate this automatically, so make sure that the setting is the same on both ends.
9. Click **Save Changes**.

Setting up third-party IPsec clients

With the large number of IPsec servers available, configuration parameters cannot be provided for each device. The following information does, however, provide the best configuration for enabling a Lotus Foundations server to create a virtual private network (VPN), with third-party devices.

Lotus Foundations setup

For a Lotus Foundations setup, use these configurations:

- **Remote server** - Enter the external IP address of the remote unit.
- **Remote subnet** - Enter the internal IP address of the remote unit and the subnet. For example, if the unit's internal IP address is 192.168.10.1 with a subnet mask of 255.255.255.0, enter 192.168.10.0/24.
- **Remote IKE key** - Enter your shared key that is being used.
- **Key Type** - Select PSK.
- **Perfect Forward Secrecy (PFS)** - Select Yes.

Third-party IPsec client setup

For a third-party setup, use these configurations:

- **Encryption / Tunnel** - 3DES and MD5.
- **Security Association (SA) Lifetime** - set to 3600 seconds.
- **Mode** - If there are different modes available, select Main Mode.
- **Private Key Secret** - Use preshared secret keys (PSK), not RSA keys or other keys such as PKI, as these are not supported on Lotus Foundations.
- **Perfect Forward Secrecy** - Perfect Forward Secrecy (PFS) must be enabled on both ends of the connection. The IPsec protocols do not provide a method for the two ends to negotiate this, so you must ensure it is set correctly.

Remote access services

What is RAS?

Remote Access Services (RAS) is a feature that enables you to access an internal network while at home or on the road. You can take advantage of RAS with the following:

- A virtual private network (VPN), which requires the Internet and a Point-to-Point Tunneling Protocol (PPTP) client
- A dial-in connection (which requires a dial-up modem and a phone line)

Windows typically has a PPTP client built-in. You might have to purchase a separate software package if you are using a Macintosh.

To establish a remote connection, users must have PPTP or dial-in access. Refer to the “*Creating users*” on page 30 section in the User & Team Management chapter for more information.

PPTP - client-to-server VPN service

Configuring VPN service on Lotus Foundations

To configure the virtual private network (VPN) service on Lotus Foundations, perform these steps:

1. Click **VPN** in the left side menu of WebConfig. The **VPN Setup** tab of the VPN Setup page is displayed.
2. In the **PPTP Server** field, select **Enable** to enable the Point-to-Point Tunneling Protocol (PPTP) server.
3. Click **Save Changes**.

Configuring VPN service in Windows

Before you can establish a VPN connection, you have to install VPN service on a Windows 95/98/Me workstation. Windows 2000, Windows XP, and Windows Vista workstations already have VPN services installed.

1. Click **Start** → **Settings** → **Control Panel**. Double-click the **Add/Remove programs** icon.
2. The Add/Remove Programs Properties window is displayed. Select the **Windows Setup** tab.
3. Select **Communications** from the **Components** list and click **Details...** A second **Components** list is displayed, showing the communications components that are already installed and those that can be installed.
4. Scroll to **Virtual Private Networking** in the **Components** list.
 - If it already has a check, then VPN software has already been installed. Proceed to “*Establishing a VPN connection*”.
 - If it does not have a check, you must install the VPN software. Proceed to the next step.
5. Select **Virtual Private Networking** and click **OK**.
6. The Windows Setup window is displayed again. Click **Apply**. The software is installed automatically.
7. Reboot the computer when the software is finished installing.

You might be asked to insert your Windows 95/98/Me disk for additional software components to be loaded. Follow the instructions provided, and refer to Microsoft Support for more information.

Establishing a VPN connection

To establish a VPN connection to a Lotus Foundations server, you need to know your username and password and the Lotus Foundations server’s domain name or Internet Protocol (IP) address.

Windows 2000/XP/Vista

To establish a VPN connection on a Windows 2000, Windows XP, or Windows Vista machine, follow these steps (these steps vary slightly for Windows XP and Windows Vista):

1. In Windows, go to **Network Connections**.
2. Select **New Connection Wizard** and click **Next**.
3. In the Network Connection Type window, select the **Connect to the network at my workplace**, then click **Next**.
4. In the following Window, select **Virtual Private Network connection**, then click **Next**.
5. In the Connection Name window, enter a name for the location to which you are connecting.

6. In the Public Network window, select **Do not dial the initial connection** and click **Next**.
7. In the VPN Server Selection window, enter the public IP address of the Lotus Foundations server, or enter the host name followed by the domain name. Click **Next**.
8. Click **Finish**. Now that the VPN connection has been created, you need to configure the settings before connecting to the remote network.
9. Open the VPN connection. Before logging in for the first time click **Properties**.
10. Click the **Networking** tab and select **PPTP VPN** from the **Type of VPN** drop-down box. Click **OK**. This only needs to be set once for each connection.
11. Log in using the provided Lotus Foundations username and password and click **OK**. Various messages display such as *Verifying the connection...* and *Registering the user...* prior to a complete connection. You can log in through PPTP as any user on the Lotus Foundations server, so long as the user has PPTP enabled from the **Users** menu.

Windows 95/98/Me

To establish a VPN connection on a Windows 95, Windows 98, or Windows Me machine, follow these steps:

1. Select **Start** → **Programs** → **Accessories** → **Communications** → **Dial-up Networking**.
2. Double-click the **Make New Connection** icon.
3. Enter a name for the VPN connection. Click **Next**.
4. Enter your Lotus Foundations server's host name or external IP address:
 - Enter a host name (such as `www.example.com`) if Lotus Foundations provides Domain Name Service (DNS) resolution for your domain.
 - Enter an IP address (such as `192.168.0.1`) if Lotus Foundations does not provide DNS resolution. To find the external IP address, click **Local Network** in the left side menu of WebConfig, then click the **Advanced Setup** tab. In the Network Devices section of the page, locate the IP address of the untrusted Ethernet interface (usually Eth1).
5. Click **Next**.
6. Click **Finish**. You have created an icon that activates a VPN connection to your home network through your Lotus Foundations server.
7. Right-click the icon that you just created and select **Properties**. In the window that is displayed, click the **Server Types** tab.
8. In the **Advanced options** section of the screen, ensure that only the following are selected:
 - **Enable software compression**
 - **Require encrypted password**
 - **Require data encryption**
9. In the **Allowed network protocol** section of the window, ensure that only **TCP/IP** is selected. Click **OK**.
10. Once you are connected to the Internet, establish a VPN connection to the internal network by double-clicking the icon that you created in step 6. You can log in through PPTP as any user on the Lotus Foundations server, provided the user has PPTP enabled from the **Users** menu.
11. Enter your Lotus Foundations login name and password. Click **Connect**.
12. Click **Close** to minimize this window. You are now connected to your local network through a secure VPN. Depending on your Internet connection, it might take longer than normal to complete network requests. An icon showing traffic between your workstation and the Lotus Foundations server to which you are connected is displayed in the bottom right corner of the screen.
13. To end the VPN connection, double-click the icon. Select **Disconnect** in the window that is displayed.

Disconnect a PPTP connection

1. On the **Status** page of the WebConfig console, in the **Services Status** section, the **PPTP Connections** line displays the status of all PPTP connections. If there are active connections, a **Details** link is displayed.
2. Click the **Details** link. The Active PPTP Users screen is displayed.
3. Click the **Delete** action icon of the user whose PPTP connection you want to disconnect.
4. A window is displayed that asks Are you sure you want to disconnect *username*? Click **OK** to disconnect the PPTP connection.

Dial-in service

Configuring Dial-in Service on Lotus Foundations

1. Click **Dial-up** in the left side menu of WebConfig. The Dial-up Networking Setup page is displayed.
2. Click the edit icon  in the Action column for the appropriate modem.
3. A second Dial-up Networking Setup page is displayed.
4. In the **Allow Dial in connections** field, select **Yes**.
5. Click **Save Changes**.

Configuring Dial-in Service in Windows

1. Click **Start** → **Settings** → **Control Panel**. Double-click the **Add/Remove programs** icon.
2. The Add/Remove Programs Properties window is displayed. Select the **Windows Setup** tab.
3. Select **Communications** from the **Components** list and click **Details....** A second **Components** list is displayed, showing the communications components that are already installed and those that can be installed.
4. Select **Dial-Up Networking** from the **Components** list.
 - If it is already selected, then dial-in software has already been installed. Proceed to “*Establishing a dial-in connection*”.
 - If it is not selected, you must install the dial-in software. Proceed to the next step.
5. Select **Dial-Up Networking** and click **OK**.
6. The **Windows Setup** window is re-displayed. Click **Apply**. The software is installed automatically.
7. Reboot your computer when the software is finished installing.

You might be asked to insert your Windows disk for additional software components to be loaded. Follow the instructions provided by the operating system during this process.

Establishing a dial-in connection

When a user dials into the Lotus Foundations server, their username is displayed in the **Internet Status** field in the **Services Status** section of Status page in the WebConfig console for the duration of the connection. The administrator can choose to terminate the user’s connection from this page.

To establish a dial-in connection to your network, you need to know your Lotus Foundations user ID and password and the phone number of a modem that is connected to an external phone line. Depending on your Internet connection, it might take longer than normal to complete network requests.

To establish a dial-in connection on a Windows 95, Windows 98, or Windows Me machine, follow these steps:

1. Select **Start** → **Programs** → **Accessories** → **Communications** → **Dial-up Networking**.
2. Double-click the **Make New Connection** icon.
3. Enter a name for the dial-in connection. Click **Next**.

4. Enter your area code, phone number, and country code.
5. Click **Next**.
6. Click **Finish**. You have created an icon that activates a dial-in connection to the internal network.
7. Establish a dial-in connection by double-clicking the icon that you created in the previous step.
8. Enter your Lotus Foundations login name and password. Click **Connect**. A window showing you the progress of the connection is displayed. An icon showing traffic between your workstation and the Lotus Foundations server to which you are connected to is displayed in the bottom right corner of your screen when you are connected to the local network.
9. To terminate the connection, double-click the icon. Select **Disconnect** in the window that is displayed.

Terminating a connection from WebConfig

When a user dials into the Lotus Foundations server, their username is displayed in the **Internet Status** field in the **Services Status** section of Status page of WebConfig for the duration of the connection. The administrator can choose to terminate the user's connection from this page.

Firewall services

The firewall subsystem featured in Lotus Foundations is entirely auto-configuring and automatically reconfigures its parameters to adapt to any Lotus Foundations server settings. There are no user controls needed. However, you can choose to restrict outgoing traffic and view a log of all requests to traverse the firewall.

Traffic denied inbound

The firewall denies all inbound network traffic that is not for the following:

- Remote administration
- Private network hosts
- Service network hosts
- The firewall itself

Traffic permitted inbound

The firewall supports access requests for the following services, if enabled.

- File Transfer Protocol (FTP) - Active and Passive Mode
- Hypertext Transfer Protocol (HTTP)
- Hypertext Transfer Protocol Secure (HTTPS)
- Simple Mail Transfer Protocol (SMTP)

See "Log messages" on page 129 for what firewall request information is logged.

Traffic permitted outbound

Lotus Foundations permits the following protocols through the firewall.

Table 14. Permitted protocols through the Lotus Foundations firewall

| Protocol - Transport Layer Protocol/Port | Transport Layer Protocol - Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) | Port | Purpose |
|--|--|------|---|
| Telnet | TCP | 23 | Access resources on a UNIX/Linux computer |

Table 14. Permitted protocols through the Lotus Foundations firewall (continued)

| | | | |
|--|-------------|-------|--|
| File Transfer Protocol (FTP) | TCP | 20–21 | Copy files between computers |
| Hypertext Transfer Protocol (HTTP) | TCP | 80 | Make Web pages available over the Internet |
| Hypertext Transfer Protocol Secure (HTTPS) | TCP | 443 | Make secure Web pages available over the Internet |
| Simple Mail Transfer Protocol (SMTP) | TCP | 25 | Transfer or send e-mail messages between servers |
| Domain Name Service (DNS) | TCP and UDP | 53 | Navigate the Internet using domain names instead of IP addresses |
| Post Office Protocol version 3 (POP3) | TCP | 110 | Read e-mail from a single inbox |
| Internet Message Access Protocol (IMAP) | TCP | 143 | Read e-mail from a remote location |

All other non-Remote Administration traffic from private, service, and public network clients directed to or through the Lotus Foundations firewall is dropped or denied.

This feature is disabled as the default setting for Lotus Foundations. Once the feature is enabled, users within your network cannot use programs that do not adhere to the above protocols, such as ICQ.

To enable the Restrict Outgoing Traffic option, follow these steps:

1. Click **Local Network** in the left side menu of WebConfig. The **Basic Setup** tab of the Local Network Options page is displayed.

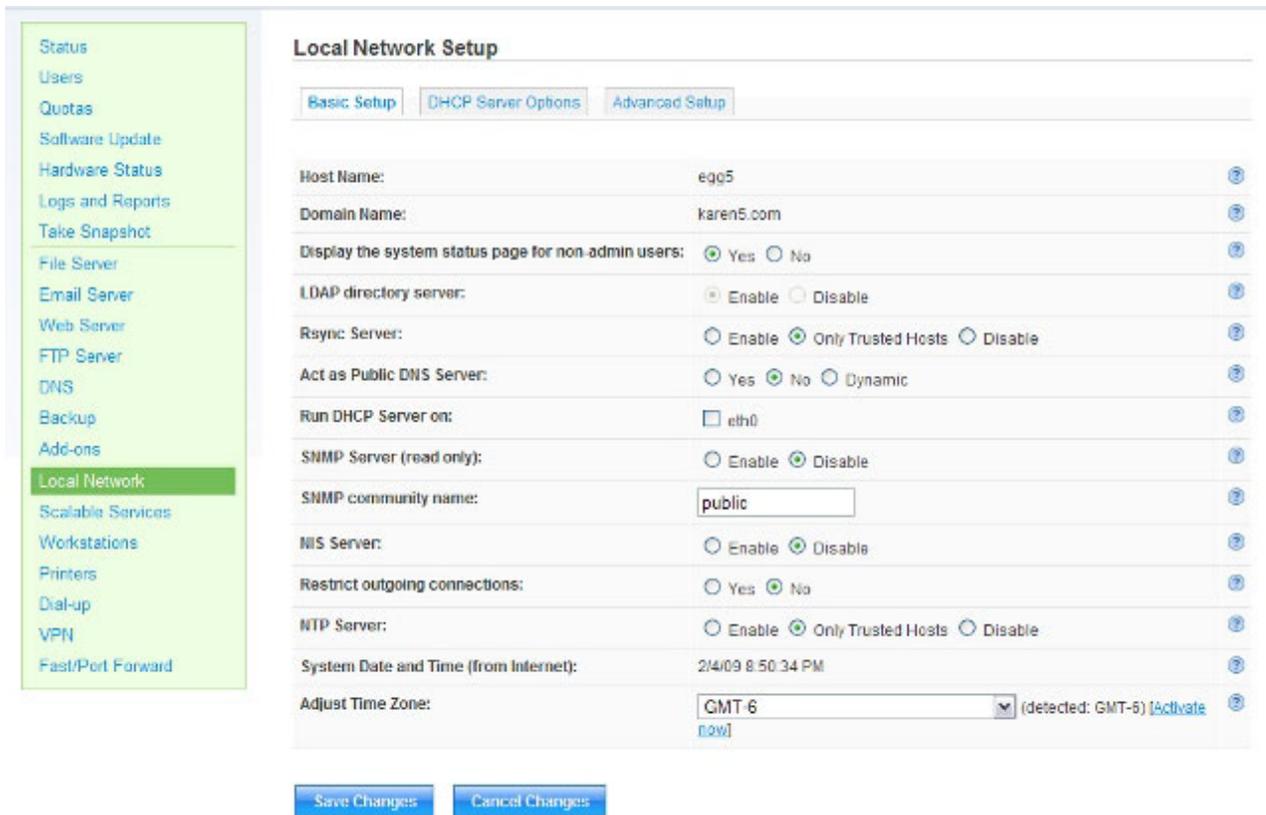


Figure 42. Basic Setup tab of the Local Network Setup page of WebConfig

2. In the **Restricts outgoing connections** field, select **Enable** to configure Lotus Foundations to only enable the above outbound ports. Select **Disable** to enable all outgoing traffic.
3. Click **Save Changes**.

Restricting outgoing traffic helps to block applications such as MSN Messenger, Yahoo Messenger, Kazaa, Morpheus, and similar applications.

Firewall log

See the “Log messages” on page 129 chapter for information on firewall logs.

Domain Name Service

What is DNS?

Domain Name Service (DNS) is the protocol used to convert Internet domain names into Internet Protocol (IP) addresses. If DNS is configured, users can access information on the local network and the Internet using domain names instead of specific IP addresses.

Configuring DNS services can be complicated because it often requires dealing with outside organizations called domain registrars. If you are uncertain about issues related to DNS, ask your Internet service provider (ISP) to help you.

DNS Services

Lotus Foundations runs two different kinds of services for Domain Name Service (DNS):

- **DNS Lookup and Caching Server:** This server converts domain names (such as `www.ibm.com`) into Internet Protocol (IP) addresses and then sends the IP addresses to your browser. Lotus Foundations

runs the DNS lookup and caching server on your local network and blocks connections to the lookup server from the Internet. There are no special options to configure the DNS lookup and caching server.

- **DNS Publishing Server:** This server adds names for your own network (such as `www.example.com`) into the global DNS system so that people can find your IP address to access your Web site or to send you email. The DNS publishing server and how it can be configured is explained in the rest of this chapter.

Configuring Public DNS

This public Domain Name Service (DNS) option only controls the DNS publishing server and how people outside your local network communicate with it. The DNS publishing server is always active for computers on your local network.

To configure the public DNS, follow these steps:

1. Click **Local Network** in the left side menu of WebConfig. The **Basic Setup** tab of the Local Network Options page is displayed.
2. In the **Act as Public DNS Server** field, select one of the following options: **No**, **Yes**, or **Dynamic**.
 - If you do not want to publish any DNS entries, select **No**; this is the default setting.
 - If you want to provide services to the outside world, such as e-mail, you must enable the DNS server by selecting **Yes** or **Dynamic**.
 - Your choice depends on some relatively complex issues involved in domain name registration.
3. Click **Save Changes**.

How the DNS system works

DNS hierarchy

The Internet Domain Name Service (DNS) server network is arranged as a hierarchy, in which a single root domain, sometimes called dot (`.`), links to the set of top-level domains, such as `.com` and `.org`. Each of the top-level domains contains a link to each of the second-level domains, such as `ibm.com` and `mydomain.org`. Third- and fourth-level domains are less common and are used in large organizations like universities.

You most likely publish a second-level domain name such as `example.com`. When you do that, your DNS server, if enabled, automatically publishes the names inside `example.com`, such as `www.example.com` and `mail.example.com`.

Domain registrars

However, there is still a part that must be done manually. In this example, you have to create a link on the `.com` server to ask your second-level domain to be referred to your Lotus Foundations server's Internet Protocol (IP) address. To do this, you need to visit a domain registrar to make sure that your domain name is not already being used by someone else, as well as to give them the outside IP address of your Lotus Foundations server.

To register a domain name, your Lotus Foundations server must have a static IP address. Most Internet service providers (ISPs) provide this service for an additional fee. Dynamic DNS (DDNS) can be used in place of a static IP address. Refer to *"Dynamic DNS" on page 103* in this chapter for more information.

When you enable your public DNS server and register with a domain registrar, people should be able to look up the IP address associated with your domain name. To test this, follow these steps:

1. Click **Web Server** in the left side menu of WebConfig.
2. Select **Yes** in the **Enable Web Server** field of the **Basic Setup** tab.
3. Ask someone outside the local network if they can view your domain.

Dynamic DNS

Dynamic DNS is a Lotus Foundations feature that enables you to publish Domain Name Service (DNS) entries and provide Internet services even if you have a dynamic Internet Protocol (IP) address, as opposed to a static IP address.

When you register your domain with a registrar, you give them the address of the primary server and backup server, which already have static IP addresses. When your Lotus Foundations server connects to the Internet, it automatically informs the servers about your current IP address and asks them to publish your up-to-date DNS information.

You need to provide a domain registrar with the following DNS server addresses:

1. dyndns1.ivivanet.com
2. dyndns2.ivivanet.com
3. dyndns3.ivivanet.com

After you provide a domain registrar with the address of your primary and backup servers, you then need to set your public DNS server to **Dynamic**. Lotus Foundations does the rest of the configuration automatically.

Manually creating DNS entries

Based on the services you have enabled, Lotus Foundations automatically decides which Domain Name Service (DNS) names to publish. For example, if your domain name is `example.com`, and the **Enable Web Server** option is set to **Yes** (not **Trusted Hosts Only**), then Lotus Foundations automatically publishes the DNS name `www.example.com` as a pointer to your Web server. Similarly, if you enable the Simple Mail Transfer Protocol (SMTP) e-mail delivery server, it publishes the name `mail.example.com`.

Although Lotus Foundations publishes names automatically, you might want to occasionally add extra names to your DNS server. You might also want to add an entry that enables people to access your site without typing `www.` before the address.

Changing DNS information with a domain registrar can often take 24 - 72 hours to replicate through the DNS backbone.

Types of DNS entries

You can create four kinds of DNS entries:

- **A (address)**: Creates an entry for converting a name (such as `www.example.com`) to an Internet Protocol (IP) address (such as `111.22.33.44`). This is the most common type of entry.
- **NS (copy from nameserver)**: Enables you to mirror someone else's DNS server. Every DNS server should have a backup server with an additional copy of the data. When you register a domain name, the registrar generally asks for a primary and a secondary server. If someone asks you to act as their secondary DNS server, you can add their domain name and primary server's IP address as an NS entry.
- **MX (mail exchanger)**: Occasionally, you might want to publish a Web server and a mail server with the same name but different IP addresses. For example, you might want people to reach you by e-mail when they send to `user@example.com`, but you might want the `example.com` Web server to point to a different address. To do that, you would add address records for `example.com` and `www.example.com` pointing to your Web server, and then you would add an MX entry for `example.com` pointing to your mail server. You do not need to create a separate MX entry if it points to the same address as the address record.
- **DR (dynamic redirect)**: Dynamic redirection can be used to circumvent blocked HTTP (Hypertext Transfer Protocol, or Web) ports. Any Web requests directed to the address entered as *Name* are

automatically redirected by a Dynamic DNS server to port 4201 on the site entered as *Value*. This is almost transparent for clients, who only notice that the host name and port have changed slightly.

Creating a DNS entry

To create a private DNS entry, follow these steps:

1. Click **DNS** in the left side menu of WebConfig. The **Public Entries** tab of the DNS Entries page is displayed.
2. To list, create, or edit your private DNS entries, click the **Private Entries** tab.
 - Private DNS entries are available only to the internal network and include host names of all the computers the Lotus Foundations server can find on the local network.
 - Public DNS entries include the mail exchange (MX) record and entries for the untrusted (external) network interface. Virtual Web server DNS records also go on the public DNS list.
 - Most of the listings, both public and private, are automatically set up by Lotus Foundations.
3. To add a private DNS entry, click **Add Private Entry**. The Add DNS Entry page is displayed.
4. In the **Name** field, enter a name for the entry.
5. In the **Entry Type** field, select one of the following: **Copy from Nameserver (NS)**, **Mail Exchanger (MX)**, **Address (A)**, or **Dynamic Redirect (DR)**.
6. In the **Value** field, enter the target IP address.
7. Click **Save Changes**.

Editing an existing DNS entry

To edit an existing private DNS entry, follow these steps:

1. Click **DNS** in the left side menu of WebConfig. The **Public Entries** tab of the DNS Entries page is displayed.
2. To edit your private DNS entries, click the **Private Entries** tab.
3. Click the edit icon  in the Action column for the entry. The **Modify DNS Entry** page is displayed.
4. Make the appropriate changes and click **Save Changes**.

Workstation viewer

What is the workstation viewer?

The workstation viewer is a Lotus Foundations subsystem that can list the workstations and servers that are connected through the local network. The Workstations page tells you which computers are on the network, their names and Internet Protocol (IP) addresses, and who is logged on.

If a workstation can be administered remotely using virtual network computing (VNC), the remote administration program can be accessed from WebConfig.

Accessing the workstation viewer

To access the workstation viewer, follow these steps:

1. Click **Workstations** in the left-side menu of WebConfig. The Workstations page is displayed.
2. Scanning for workstations can waste bandwidth; no workstations are displayed in the list by default. Click **New Scan** to view an updated list of workstations.
3. Click **Refresh** after a few seconds to view the updated list. Workstations are displayed in the list if they are connected to the network. **Refresh** changes back to **New Scan** when the scan is complete.
4. Workstations can be sorted by **IP Address** or **Workstation Names** by clicking the appropriate column title.

Virtual network computing (VNC)

Using free Windows software called Virtual Network Computing (VNC), you can configure Windows, Macintosh, and UNIX workstations so they can be controlled remotely from a central workstation. If users need help or settings need to be changed, the VNC software provides an alternative to an administrator having to physically go and sit in front of the workstation to solve the problem.

Computers with a VNC remote administration server installed are displayed with the words **Remote Admin** next to them on the Workstations page.

Configuring VNC

There are two parts to configuring remote administration:

1. **VNC Server** - Should be installed on every user's workstation.
2. **VNC Viewer** - Should be installed on the administrator's workstation.

Once the servers and viewers are configured, clicking the **Remote Admin** link on the Workstations screen connects you to the remote virtual network computing (VNC) server and displays the remote desktop.

Configuring the VNC server

To configure the VNC server, perform these steps:

1. To download VNC, go to one of the following sites:
 - <http://www.realvnc.com/products/download.html>
 - <http://download.cnet.com/> (search for VNC)
 - <http://www.chromatix.uklinux.net/vnc/> (Macintosh version)
2. The file comes in a zipped format. Unzip the file in a temporary location for installation. Run the Setup program and follow the instructions. Accept all defaults during the installation process.
3. When the installation is finished, reboot the workstation.
4. Click **Start** → **Applications** → **VNC** → **Start VNC (App mode)**.
5. The first time you start VNC you have to set up a password, which is needed to connect to your workstation.
6. When VNC is active, a small VNC icon displays in the bottom right corner of your screen.

Configuring the VNC viewer (for the administrator's workstation)

To configure the VNC viewer, perform these steps:

1. Download VNC from the Internet and configure the VNC server.
2. Look for `vncviewer.exe` and copy it to an easily navigable location, such as `C:\Windows`.
3. Click **Start** → **Programs** → **Windows Explorer**.
4. From the **Tools** menu, select **Folder Options**.
5. Click the **File Types** tab. The File Types window is displayed.
6. Click **New Type...** The Add New File Type window is displayed.
7. Enter a description of the file type (such as VNC Viewer Admin) in the **Description of Type** field.
8. Enter `vnc` in the **Associated extension** field.
9. Enter `application/x-vnc` in the **Content Type (MIME)** field.
10. Click **New**. The New Action window is displayed.
11. Enter `open` in the **Action** field.
12. Enter the following line in the **Application used...** field: `c:\windows` refers to the location where VNC has been installed. The quotations around "%1" are required.
`c:\windows\vncviewer.exe /config "%1"`

13. Click **OK**. VNC Viewer Admin is displayed in the Registered file types list of the File Types screen.

Fast/Port Forward

What is Fast/Port Forward?

The Fast/Port Forward technology in Lotus Foundations enables you to forward Internet traffic from a specific address and interface to another address and interface. A subsystem that performs this function is usually called a proxy server.

When computers on the Internet access services on your internal, protected network, they "talk through" your Lotus Foundations server. Fast/Port Forward makes sure that these untrusted computers can only access the information and services that you want them to access.

If Fast/Port Forward is disabled, no one can see anything on your local network because Lotus Foundations acts as a firewall. If you enable Fast/Port Forward, you are making a protected "hole" in your firewall that enables computers on the outside to access your network. To decide whether you want to use Fast/Port Forward, you need to decide if enabling Fast/Port Forward is worth the added security risk.

Note: Because you are affecting the firewall security of your network, it is very important that you understand what you are doing while configuring Fast/Port Forward.

Fast/Port Forward belongs to a class of programs known as proxy servers. It is the Lotus Foundations inbound proxy server. Its job is to accept Transmission Control Protocol (TCP) or User Datagram Protocol (UDP) connections on one address and port, then forward them off to some other address and port. There are many programs that do this, but Fast/Port Forward provides simplified configuration, uses less memory, and is generally faster than any other solution. It uses zero-forking technology to keep its resource usage to a minimum while still running faster than most other proxies.

Introduction to TCP/IP

Each computer on the Internet must have a unique Internet Protocol (IP) address. Network protocols come in layers and IP is just one of those layers. The job of IP is to get data, split it into small chunks called packets, and then transport those packets from one computer to another on the Internet.

When the computer receives an IP packet, it needs to figure out what service it belongs to and which open connection in which it is involved. For that, it uses two higher-level protocols known as Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). TCP and UDP introduce port numbers that specify where the data is supposed to go and how the computer is supposed to handle it.

Fast/Port Forward can handle both TCP and UDP. It processes them differently from each other, but you do not need to worry about this for configuration purposes.

User Datagram Protocol (UDP)

Using UDP is very much like sending a telegram. You receive a message, and you can send a reply. The Domain Name Service (DNS) mentioned earlier uses UDP. One computer sends a message asking to translate a name (for example, `www.example.com`) into a number. The answering DNS server sends a message saying that the IP address of `www.example.com` is `192.168.1.1`.

Transport Control Protocol (TCP)

Using TCP is very much like making a telephone call. A person calls you, and you answer. You go through an introductory sequence, you have a conversation, and then you finish the call (or in TCP

terminology, you close the connection). TCP is used for more complicated network tasks, such as Web browsing.

Proxy servers

Lotus Foundations acts as a firewall, meaning that it blocks computers on the Internet from having access to your private servers.

If you want to make a service available to the outside world, Fast/Port Forward controls the connection for you. When someone outside wants to access the service, they send the request to a port on your Lotus Foundations server. Fast/Port Forward then connects them to the service. This process has two connections: one from the client to the Lotus Foundations server, and another from the Lotus Foundations server to the service. When either the client or the server transmits information, Lotus Foundations forwards it to the opposite end of the connection.

As a result, you need to know the addresses and port numbers of both the source of the information and the destination of the information. Lotus Foundations receives connection requests from the source address and forwards them to the destination.

If you want to use Fast/Port Forward, you probably already have a clear idea of what your destination address is. The source, however, might be more difficult to determine and ultimately depends on how your Internet Protocol (IP) address is configured.

Static and dynamic IP addresses

A person trying to access Fast/Port Forward services through your Lotus Foundations server must know your assigned IP address to locate you on the Internet. Each time you connect to the Internet, your Internet service provider (ISP) assigns you an IP address. Dynamic IP addresses are inconvenient for use with Fast/Port Forward because your address changes each time you connect, making it difficult for your clients to find you.

If you specifically ask for one, your ISP can give you a static IP address (static IP addresses do not change). Once you have a working static IP address, you can add it to a Domain Name Service (DNS) server, which converts your domain's readable name into its IP address.

Configuring Fast/Port Forward

You can configure Fast/Port Forward once you know your source and destination addresses. If you still are not sure where the addresses come from, a few examples are displayed in *"Forwarding scenarios"* on page 109.

Note: Remember that you decrease firewall security when you enable Fast/Port Forward.

1. Log in to WebConfig with your administrator username and password.
2. Click **Fast/Port Forward** in the left side menu of WebConfig. The Fast Forward Setup page is displayed, showing the list of addresses being forwarded. This list might be empty if no addresses are being forwarded.

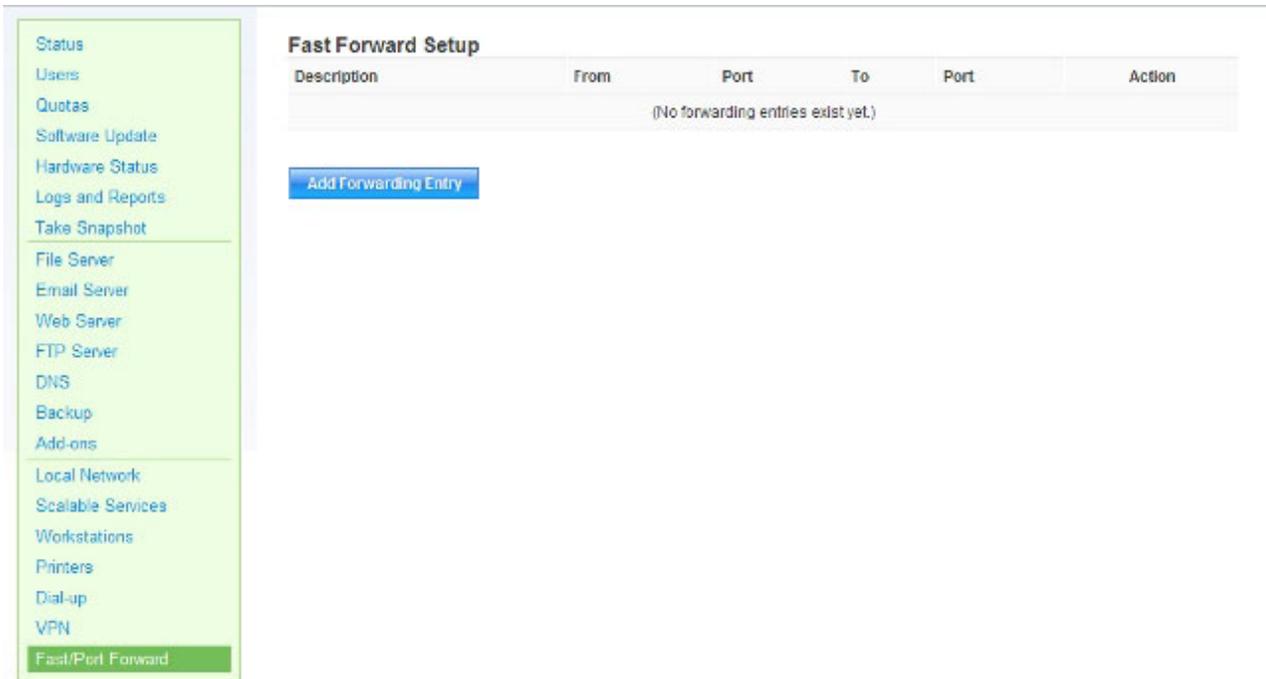


Figure 43. Fast Forward Setup page of WebConfig

Creating a new forward

To create a new forwarding entry, follow these steps:

1. Click **Add Forwarding Entry**. The Add Forward page is displayed.

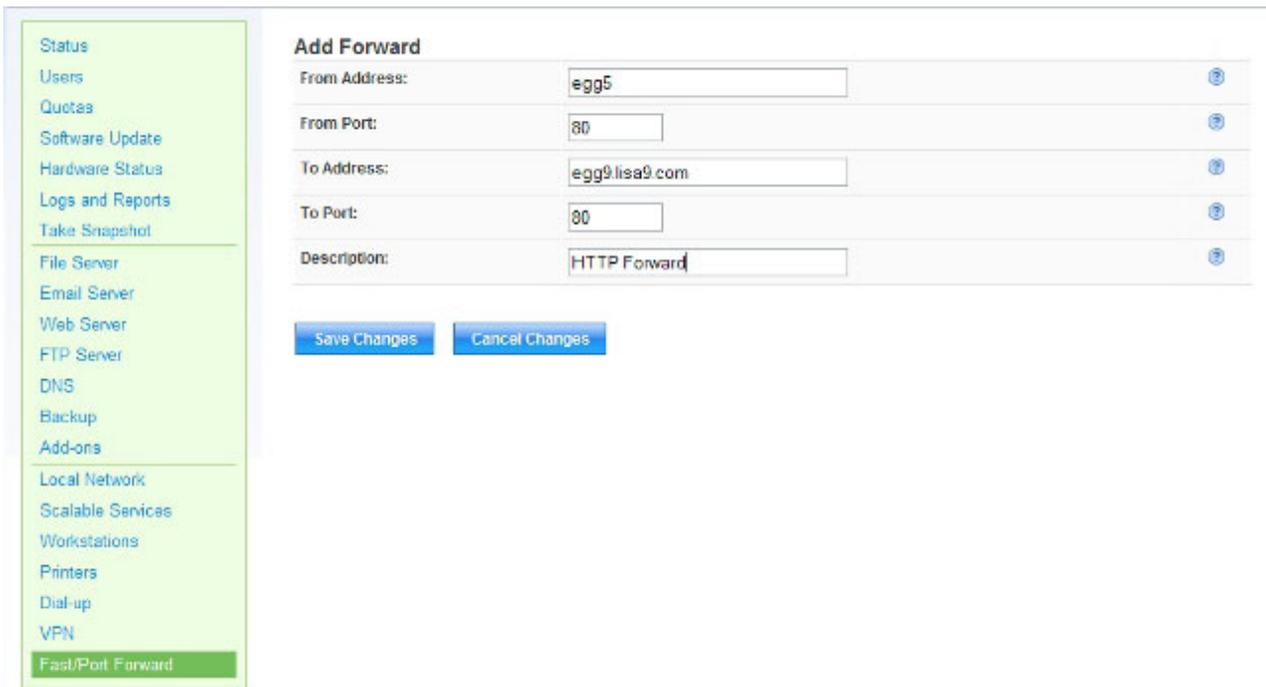


Figure 44. Add Forward page for Fast/Port Forward

2. Enter the source address and port number in the **From Address** and **From Port** fields. You can only attach one forward connection to any given source address and port.
3. Enter the destination address and port number in the **To Address** and **To Port** fields. Ensure that you have entered the destination information correctly. If you forward connections to a server that is not answering, Fast/Port Forward drops the connection.
4. Enter a description of the Fast/Port Forward to keep track of its purpose or destination.
5. Click **Save Changes**.

Editing a forward

To edit a forwarding entry, follow these steps:

1. Click **Fast/Port Forward** in the left side menu of WebConfig.
2. On the Fast/Port Forward page, click the edit icon  for the appropriate forward. The Modify Forward page is displayed.
3. Change the appropriate source or destination information.
4. Click **Save Changes**.

Deleting a forward

To delete a forwarding entry, follow these steps:

1. Click **Fast/Port Forward** in the left side menu of WebConfig.
2. On the Fast/Port Forward page, click the delete icon  for the appropriate forward.
3. To confirm the deletion, click **OK** in the pop-up window that is displayed.

Forwarding scenarios

Below are a few common forwarding examples:

1. Your internal network has an e-mail server called Fred running Windows NT. The address of the server is 192.168.1.5. Set the source address to `host_name` and the source port to 25, which is the Simple Mail Transfer Protocol (SMTP) port. Set the destination address to 192.168.1.5 and the destination port to 25. Now people can send e-mail to your Lotus Foundations server's static Internet Protocol (IP) address, and it is forwarded to your mail server.
2. If Fred has a Domain Name Services (DNS) server on port 53, you can set a forward from the source address of `host_name` and the source port of 53 to the destination address to 192.168.1.5 and the destination port of 53. People on the Internet now can look up host names that belong to your local network.
3. You can make WebConfig accessible from the outside world. An example reason of why you might want to do this is to allow technical support to access your Lotus Foundations server and help you resolve problems. Port 80 on Lotus Foundations is already in use for the company Web server, so use port 81 as the source port. WebConfig uses port 8043; if the destination IP address is 192.168.1.1, the complete destination address is 192.168.1.1/port 8043. To access WebConfig from the outside, you would need to use a special address:

`https://www.yournetwork.com:81/`

Multiple static IP addresses

In certain cases, you want Fast/Port Forward to treat connections differently depending on their target. For example, you might want e-mail from `mail1.yournetwork.com` to be sent to Fred, your NT server, and e-mail from `mail2.yournetwork.com` to be sent to Barney, your UNIX server. To do this, your Internet service provider (ISP) needs to assign you multiple static Internet Protocol (IP) addresses. Some ISPs may not offer this service.

If you have two static IP addresses (for example, 207.6.60.1 and 207.6.60.2), and you want the setup just described, follow these steps:

- Create one forwarding entry with the source address 207.6.60.1 and source port 25, and the destination address 192.168.1.5 and destination port 25.
- Create another forwarding entry with the source address 207.6.60.2 and source port 25, and the destination address 192.168.1.6 and destination port 25.

Common port numbers

A few common port numbers that you can use with Fast/Port Forward are listed in the table below.

Table 15. Common port numbers for use with Fast/Port Forward

| Port | Use |
|------|---|
| 22 | Secure Shell (SSH) |
| 23 | Telnet |
| 25 | Simple Mail Transfer Protocol (SMTP) |
| 79 | Finger |
| 80 | Hypertext Transfer Protocol (HTTP) - Web server |
| 110 | Post Office Protocol (POP) |
| 5631 | PCAnywhere |
| 443 | Web server secure port (HTTPS) |

Some ports cannot be used with Fast/Port Forward. For example, the common port number for File Transfer Protocol (FTP), port 21, does not work because it uses multiple connections that include both ports 20 and 21.

Troubleshooting Fast/Port Forward

The WebConfig page in Lotus Foundations might display the following message:

An error occurred while Fast Forward tried to bind to one or more of the addresses specified.

This message might be displayed in the following situations:

- You are trying to forward to ports that are already being used by your Lotus Foundations server (such as port 80).
- Fast/Port Forward has more than one entry trying to use the same source port and address. You cannot have more than one Fast/Port Forward entry attached to the same source.

If you see this message, turn off the server that is already using the port. For example, to forward port 80 (the port used for Web services) to another address, you would first have to shut off the Web server on Lotus Foundations.

The log messages show which Fast/Port Forward entries did and did not work.

Disk management

Some Lotus Foundations services are not enabled unless hard disks are configured through the WebConfig menu.

Disk configuration (idb and RAID)

A Redundant Array of Independent Disks (RAID) is a system of storing information that reduces risk by keeping data on two or more drives. If one drive fails, your data is still safely written and stored on another drive. You do not need to know much about RAID to configure it on your Lotus Foundations server.

Intelligent Disk Backup (idb) is a system that automatically performs backup procedures as often as every fifteen minutes without input from a system administrator. See the “Intelligent disk backup (idb)” on page 114 section in “Backup & Restore” on page 114 for more information.

If your Lotus Foundations server has one disk, then you cannot take advantage of idb or RAID. If your Lotus Foundations server has exactly two disks, you can have idb backup or a two-disk RAID array, but not both. If you have three or more disks, you can have a two or more disk RAID array and idb backup or a RAID array with all available disks and no idb backup.

Configuring your disks

1. The Disk Status section in WebConfig displays a message that disk(s) have not been configured.

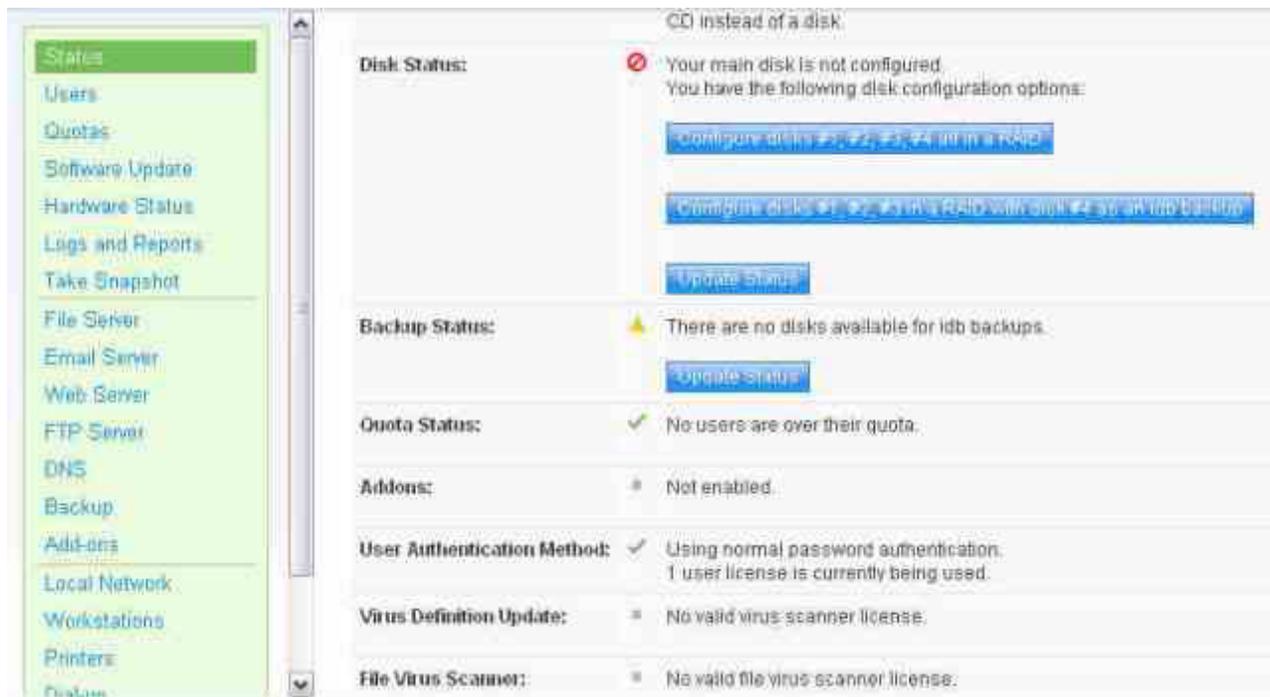


Figure 45. Disk Status section of WebConfig

2. Click the appropriate button to configure your disks.
 - For example, if you have four disks, the Disk Status section might use the following message: Your main disk is not configured. You have the following disk configuration options:
 - **Configure disks #1, #2, #3, #4 all in a RAID**
 - **Configure disks #1, #2, #3 in a RAID with disk #4 as an idb backup disk**
 - For a RAID configuration, click the **Configure disks #1, #2, #3, #4 all in a RAID** button.
 - To enable idb backup, click the **Configure disks #1, #2, #3 in a RAID with disk #4 as an idb backup disk** button.
 - If you select a RAID configuration, then the RAID array begins to rebuild. Depending on the size and number of disks in the RAID array, as well as which configuration options you choose, this process could take several hours. Rebuilding the RAID array does not noticeably affect the performance of Lotus Foundations.

Reconfiguring your disks

You can reconfigure your disk at any time. The Disk Status section of WebConfig displays your disk status and provides you with disk reconfiguration options.

Converting an idb disk to RAID

You can only convert an idb disk to part of a RAID array if your Lotus Foundations server has exactly two disks. If you have 3 or more disks, you cannot convert an idb disk to RAID.

Note: Converting your idb disk to part of a RAID array means that you will lose idb backup capabilities. In addition, the backup information that is stored on the idb disk is permanently deleted.

1. The Disk Status section of WebConfig states information about the primary disk. It then states In order to improve redundancy you can:, followed by a button labeled **Add disk #2 to your RAID array**. Click this button.
2. The RAID array then begins to rebuild. This process, which can take several hours depending upon your disk size, does not noticeably affect the performance of Lotus Foundations. Click your browser's Refresh button to view an updated status of your RAID array.
3. When the array has finished building, a message is displayed in the Disk Status section of the screen.

Converting a RAID disk to idb

If your RAID array is working correctly, you can convert a RAID disk to idb.

If you have a two-disk RAID array, you cannot convert a RAID disk to an idb disk in WebConfig.

Note: Converting your last RAID disk to idb reduces disk redundancy, regardless of how many disks your Lotus Foundations server has.

1. The Disk Status section of WebConfig has a button stating you can configure your last disk as idb. Click this button.
2. The Disk Status section of the page displays your new disk configuration.

Disk status messages

Depending on your disk configuration, one or more of the following messages are displayed in the Disk Status section of WebConfig:

Table 16. Disk Status Messages

| Message | Reason for Display |
|--|--|
| The RAID array is rebuilding. Please do not add or remove any disks until this process is finished. (% complete) | A RAID array needs to build itself the first time it is used, and rebuild when a new disk is added or when the power is turned off suddenly. Always click Shutdown before turning off your Lotus Foundations server. Failure to do so means that your RAID array needs to rebuild when you turn the server back on. Although this process does not noticeably affect the performance of Lotus Foundations, it can take several hours to complete depending on the size and number of disks in your array. |
| Your disk array is working correctly. | A RAID array is finished building. |
| No disks detected! Are your drives inserted or locked? | Your drives are not fully inserted and properly locked or when all available drives have crashed. If your drives are not locked, insert the hard disk key into the lock and turn it clockwise until it snaps back into the locked position. If your disks have crashed, refer to "Recovering from disk failure" on page 113 for information on how to replace failed disks. |
| The RAID array is in degraded mode. If you remove a disk, you lose access to your files. | You are missing one configured drive in a RAID array. You can create a proper RAID array by configuring a second disk. |

Table 16. Disk Status Messages (continued)

| | |
|--|---|
| The primary disk is in standalone mode. If you remove the disk, you lose access to your files. | You have a single disk drive, you are not using RAID, or your two-disk RAID array is in degraded mode. |
| There is no disk available for idb backup. | No configured idb disk is present in the system. |
| Disk #_ is being used for Intelligent Disk Backup (idb). | The last disk is used for idb instead of as part of a RAID array. |
| You can add disk #_ to your RAID array to improve redundancy. | You have at least one unconfigured disk or if your last disk is being used for idb. Click the link to add the disk to the RAID array. |
| You can configure disk #_ for use in idb backups. | The last disk drive is unconfigured. The previous message also displays, but you can only choose one of the options. |
| There is no reason to use disk #_. | Any extra disks in the system that cannot be used. This occurs when the RAID array is complete, and there is already an idb disk. |
| Disk #_ is too small to be added to the RAID array. | Any unconfigured disks that are too small to fit into the RAID. To solve this problem, turn the server off and replace the disk with a larger disk. |
| Disk #_ cannot be used until a RAID license is purchased. | A system has three or more disks installed, but the system does not have a RAID license. To solve this problem, either remove the disk or purchase a RAID license for the system. |

Recovering from disk failure

If one of the disks in your RAID array fails, follow these steps:

1. Power down the server.
2. Turn off the main power on the server.

Note: The button for the main power button on the Lotus Foundations Appliance is below the control panel on the front of the Lotus Foundations Appliance. This is different from the power button in the upper left corner of the Lotus Foundations Appliance.

3. Remove the hard disk and replace it with a new one as soon as possible. See “Installing a new hard drive” on page 114 for more information.
4. If applicable, turn the main power switch back on.
5. Press the power button.
6. Connect to WebConfig and log in.
7. The Disk Status section of the Status page of WebConfig presents you with up to two options:
 - To configure the new disk as part of the existing RAID array, click **Add disk #_ to your RAID array**.
 - To configure the new disk as idb, click **Configure disk #_ for use in idb backups**.
8. Depending on your choice, Lotus Foundations configures the new disk as the idb disk or as part of your RAID array.

Hard disk failure

If your problem is a hard disk failure, you need the following to restore your Lotus Foundations server:

- **Last Backup** - The last backup from which you can recover data. All changes to system configuration, user files, and new files created by users since the last backup are not recoverable.
- **New hard disk** - A new hard disk drive to replace the failed hard disk drive.

Installing a new hard drive

1. Shut down the server completely. If your server has a main power switch, turn off the main power switch. Unplug the power cord.

Note: The button for the main power button on the Lotus Foundations Appliance is below the control panel on the front of the Lotus Foundations Appliance. This is different from the power button in the upper left corner of the Lotus Foundations Appliance.

2. Remove the disk from the unit.
3. Insert a new hard disk into the drive.
4. Insert your idb cartridge. Skip this step if your idb disk is already in.
5. Plug the power cord back in. If your server has a main power switch, turn the main power on.
6. Press the power button.
7. Configure the new disk in WebConfig. See the “Configuring your disks” on page 111 section of “Disk configuration (idb and RAID)” on page 110.
8. Initiate a restoration from WebConfig. See the “Backup & Restore” chapter. The length of the restore process depends on the size of your hard disk and the amount of data that has to be restored. The entire process can take up to several hours.

Note: Restoration is not necessary when adding a disk to a degraded RAID.

Backup & Restore

Intelligent disk backup (idb)

Lotus Foundations takes a different approach to backup with intelligent disk backup (idb) technology, which is both cheaper and easier to use than conventional tape backup systems. The capacity of the idb backup unit varies.

The idb system automatically performs backup procedures without input from a system administrator. However, at any time you can turn off an idb job, pause or change an idb job schedule, or manually initiate a backup procedure. Refer to “Initiating an idb backup” on page 120 for more information.

idb is available when you have a valid idb license and the Lotus Foundations disk is configured for idb backups.

Features of idb

Instead of conventional backup tapes, idb uses a removable high-capacity hard disk, which provides the following advantages:

- **Value** - One hard disk costs less than the five backup tapes needed to maintain a tape backup system.
- **High Capacity** - The idb backup cartridge can, in most cases, store a month or more of backup history.
- **Speed** - idb backup matches and often exceeds the backup speeds achieved by the most expensive tape systems on the market.
- **Instant Access** - Regular backup tapes, like cassette tapes, are a linear medium. You must fast-forward or rewind to find information. idb technology, like a compact disc, provides almost instant access to data.
- **Backup Intelligence** - You do not need a network administrator to figure out which tapes need to be loaded and when. Lotus Foundations determines when a backup needs to be made and whether the backup should be full or incremental. This decision is based on the amount of data on the main hard disk, the amount of used space on the idb system, the compressibility of your data, and the rate at

which new data is added and current data is changed or updated. As a result, your idb system maximizes the amount of historical data that is backed up.

- **Durability** - You can back up data on the hard drive continuously without worrying that the drive might wear out.
- **Continuous Backup** - You can back up data in any sequence and as often as every 15 minutes.
- **Hot Swap** - You can add and remove idb backup cartridges while the server is running, enabling you to swap idb disks without turning the server off. Hot Swap capability is only supported on SCSI and specific IDE system configurations.

Backup jobs

When you configure Lotus Foundations to use idb, one job is automatically created. This job is named Master Job. It cannot be deleted, but it can be reconfigured. By default all users and teams are included in this backup job, with the exception of the *notes* team. The data within the *notes* team includes live Domino databases that are regularly copied to the *notesbackup* team, and thus does not need to be backed up.

When you install the Lotus Foundations Start add-on, another job is automatically created. This job is named LF Start Backup. By default, this job includes the *notesbackup* team.

Configuring idb

General configuration

The idb feature of Lotus Foundations automatically backs up your data throughout the entire day, takes care of all backup tasks for you, and notifies you through email about its progress. Although most of the idb process is automated, you can adjust several parameters that determine how and when your backups are completed.

Clicking **Backup** from the left navigation pane of WebConfig opens the main idb Backup page. The main idb Backup page consists of three main sections.

Table 17. *idb Backup page sections and elements*

| Main idb Backup page sections | Section elements | Element actions |
|-------------------------------|---|---|
| idb Status | | Lists the Backup Status of idb and the amount of idb disk space being used by backups |
| Backup Jobs | Create a new job | Creates a new backup job |
| | Backup all jobs | Runs an unscheduled backup of all backup jobs |
| | Suspend all scheduling or Resume all scheduling | Stops or resume all scheduled backups |
| | <i>List of Backup Jobs</i> | Backup jobs set up on the server; clicking the job name modifies the job |
| Disk Scan | Scan idb Disk | Scans the idb drive for backup sets; used after changing the idb disk in order to synchronize the server configuration and backup sets with the new drive |

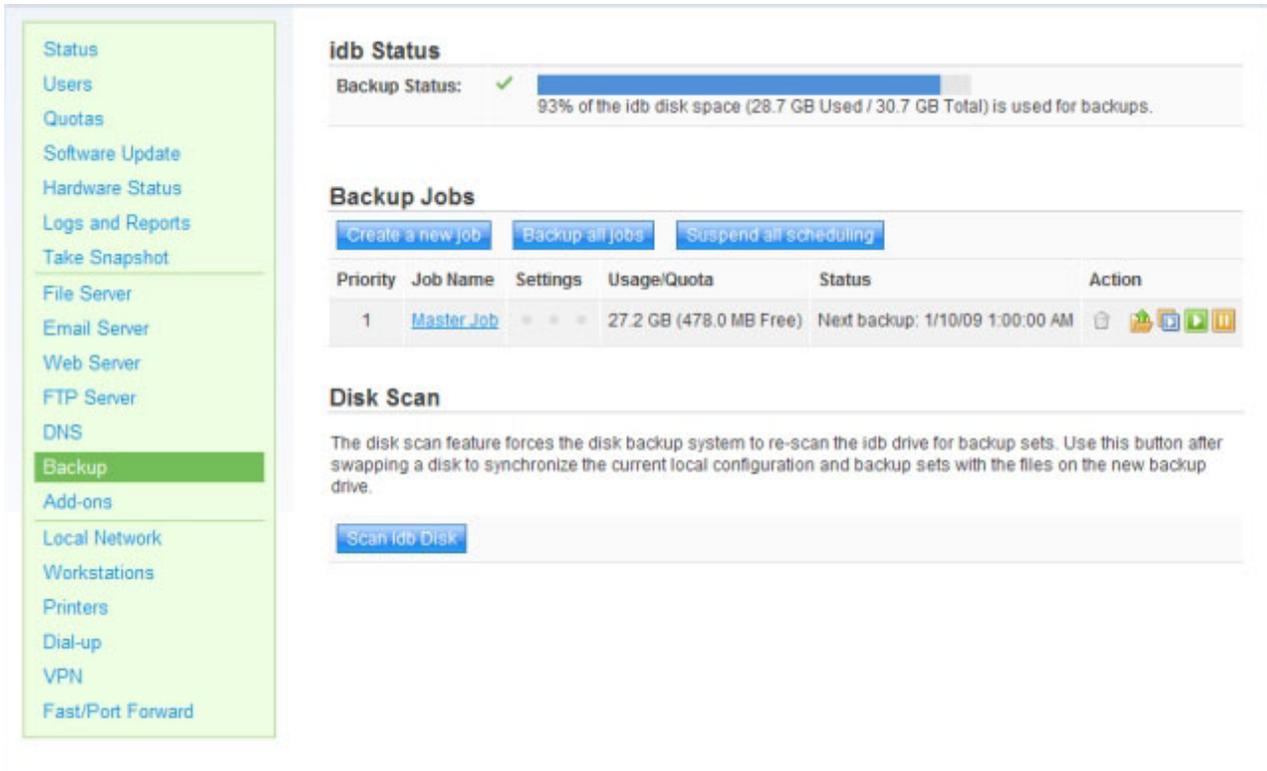


Figure 46. Main idb Backup page

Clicking the job name enables you to modify the settings for that specific backup job. The Modify Job Settings page has four tabs:

- **General**
- **Backup Files**
- **Schedule**
- **Advanced**

Note: The **Advanced** tab is only available if you have a data retention license.

Table 18 lists the specifics of the Modify Job Settings page and its tabs.

Table 18. Modify Job Settings page tabs and elements

| Modify Job Settings tab | Tab elements | Element actions |
|-------------------------|--------------|-----------------|
|-------------------------|--------------|-----------------|

Table 18. Modify Job Settings page tabs and elements (continued)

| | | |
|---------------------|------------------------------|--|
| General | Job Name | Changes the job name Cannot edit the Master Job name |
| | Priority | Assigns a unique value to the backup job; 1 is the highest priority |
| | idb Quota | Adjusts the size of the backup job |
| | Email log level | Sets the level of detail in the backup logs that are included in the backup reports; default setting is Error All message levels are available in the system logs |
| | Email backup reports to | Identifies who receives an email copy of the backup reports Enter the user ID of the administrator who should receive backup reports. If you enable the SMTP server, you can enter any email address in this field. You can also send backup reports to the Backup team to share the reports with other members of your team. See “The idb backup team” on page 119 for more details. |
| | Backup compression | Sets compression of the backup files Compressed backup files occupy less space on the idb drive, but require a longer time to back up and restore. |
| Backup Files | | Lists the directories available for backing up. If necessary, adjust these settings by clearing or selecting check boxes to set which directories are backed up in a specific job. The default setting for the Master Job is to back up all directories except the notes team. Note: Because the notes team’s data is constantly in use, it is automatically copied over to the notesbackup team, where it is safely backed up by idb. Do not enable the backup for the notes team, as this needlessly increases the time to perform backups. |
| Schedule | Full backup frequency | Backs up everything on the system |
| | Incremental backup frequency | Backs up the changes to system |
| | Daily backup at | When the daily backup is performed; select a time when nobody is using the system, such as late at night or early in the morning |
| | Weekly backup on | When the weekly backup is performed |
| | Base daily backups on | Sets the baseline backup from which the incremental backups are generated |

Table 18. Modify Job Settings page tabs and elements (continued)

| | | |
|----------|--------------------------|--|
| Advanced | Data Retention Policy | Indicates whether all teams and users use a retention policy |
| | Minimum Retention Period | Minimum amount of time the backup is retained |
| | Maximum Retention Period | Maximum amount of time the backup is retained |

Modify Job Settings

General Backup Files Schedule **Advanced**

Job Name: ?

Priority: ?

idb Quota: MB (27.1 GB Maximum) ?

Email log level: ?

Email backup reports to: ?

Backup compression: Yes No ?

Encryption: ?

Save Changes Cancel Changes

Suspend Scheduling

Figure 47. General tab of the Modify Job Settings page

idb action icons

In the Backup Jobs section of the main idb Backup page, action icons displayed to the right of a specific job control the way your backups are handled.

Table 19. idb Backup Job action icons

| idb Backup Job action icons | Icon action |
|---|--|
|  | Delete Job: Forcibly deletes any backup (and its children, if any) that is not locked; if the icon is a light gray color, the job cannot be deleted (for example, the Master Job) |
|  | Restore from Job: Browses the contents of a specific backup and restores them if necessary |
|  | Incremental Backup: Manually performs an incremental backup |

Table 19. idb Backup Job action icons (continued)

| | |
|---|--|
|  | Full Backup: Manually performs a full backup |
|  | Suspend Scheduling and Resume Scheduling: Suspends or resumes the schedule of a specific backup job |
|  | Abort: Stops a specific backup job while it is running |

The idb backup team

The *backup* team account grants all members of the team access to the Backup page in WebConfig and all associated functions. Users have full control over backups and restorations without giving them access to other administrator functions.

1. Click **Users** in the left side menu of WebConfig. The User Setup page is displayed.
2. Click the **Teams** tab. A team with the team ID *backup* and the full name *Backup Team* is created automatically.
3. To add a team or an individual user to the *backup* team, click the *backup* team's edit icon . The Modify Team page is displayed.
4. Scroll down to the **Team Members** section, click to select a team or user from the **Users & Teams** field, and then click the **Add** button. The team or user appears in the **Team Members** field.
5. To remove a user or team from the backup team, click to select the user or team from the **Team Members** field, and then click the **Remove** button.
6. Click the **Save Changes** button to save your updates and return to the User Setup page.

idb backup

Creating an idb backup job

You can create an additional backup job to the Master Job. To create a new idb backup job, follow these steps:

1. Click **Backup** in the left side menu of WebConfig. The main idb Status page is displayed.
2. Click the **Create a new job** button. The first page of the Create New Job process is displayed.
3. For **Encryption**, select if you want to encrypt the backup job and if you have a license that allows for backup encryption. If you encrypt the backup, you need to provide a password in the **Encryption Password** field. Re-enter the password in the **Encryption password (verification)** field.
4. For **Backup compression**, select if you want to compress the backup.

Note: Less space is required on the idb drive for compressed backup files, but a longer time is needed to restore files from a compressed backup.

5. Click **Next Page**.
6. For **Job Name**, type a unique name for this backup job.
7. For **Priority**, set this job to the priority you want it to have in relation to other backup jobs. The highest priority for a backup job is 1.

8. For **idb Quota**, enter the storage space on the idb disk you want this job to use. A maximum amount of storage space is listed next to the field.
9. Click **Next Page**.
10. Select which team directories you want this job to back up.

Note: The directory for the *notes* team is not included in a backup by default. It is automatically copied over to the *notesbackup* team, where it is safely backed up by idb. Enabling the backup for the *notes* team needlessly increases the time to perform backups.

11. Click **Next Page**.
12. For **Do you want this job to run automatically?**, select if you want to automatically run the backups.
13. If you choose to automatically run this job, select options for **Full backup frequency** and **Incremental backup frequency**.
14. Click **Finish**. The following message is displayed briefly: idb is performing the requested operations. Then the idb Status main page is displayed, and the new backup job is listed in the **Backup Jobs** section of the page.

Initiating an idb backup

Although the idb system automatically performs backup procedures without input from a system administrator, you can turn off idb as well as manually initiate a backup from the idb Status page.

This can also be done from the control panel found on the front of a Lotus Foundations Appliance. A backup initiated from the control panel can only restore files from the Master Job backup. It uses the settings that were last configured for the Master Job.

Note: A copy of the server configuration is made each time a backup is performed. This configuration file can be used to restore your settings in the event of a catastrophic system failure.

Initiating a backup from the WebConfig menu

1. Click **Backup** in the left side menu of WebConfig. The main idb Status page is displayed.
2. In the Backup Jobs section of the page, click the incremental backup icon  or the full backup icon , depending on the type of backup you want to run. The following message is displayed briefly: idb is performing the requested operations. Then the idb Status main page is displayed.
3. To stop the backup job before it is finished, click the abort icon .

When the backup is finished, Lotus Foundations automatically emails a backup report to the administrator.

Initiating a backup from a Lotus Foundations Appliance control panel

This can only be done with Lotus Foundations Appliances. All other hardware platforms must initiate a backup from the system's WebConfig menu.

1. Press the Backup button on the front display panel.
2. The display panel shows a 10-second countdown, during which you can stop the backup process by pressing the Cancel button.
3. After 10 seconds, the backup procedure commences and the display panel/console displays a progress bar.

4. You can delay backup for up to 24 hours by pressing the Up and Down arrows during the countdown.

idb restoration

There are four restoration scenarios:

1. **Complete System Restoration** - Upon total hard disk failure, perform a complete system restore to restore your system to the state of your most recent backup. After a complete system restoration, older copies of the existing files from the backup disk overwrite the existing files; however, new files saved to the hard drive after the backup are left untouched. Generally, you should initiate a complete system restore only when recovering from complete hard disk failure.
2. **Specific Directory Restoration** - It is possible to restore a specific user or team network directory if these files have been lost or mistakenly deleted. You can initiate a specific directory restoration only from the Backup menu. There are two types of specific directory restoration procedures:
 - **Normal Restoration** - The contents of a user or team directory are overwritten, as with a complete system restoration.
 - **Safe Mode Restoration** - The contents of a user or team directory get restored into a new subdirectory named *Restore*, which is created in the user or team directory. Users can browse through the contents of the directory from the disk, copy any needed files, and then delete the *Restore* subdirectory.
3. **Specific File Restoration** - It is possible to restore a specific user's or team's network files if they have been lost or mistakenly deleted. You can initiate a specific file restoration only from the Backup menu. There are two types of specific file restoration procedures:
 - **Normal Restoration** - The file is overwritten, as with a complete system restoration.
 - **Safe Mode Restoration** - The file is restored into a new subdirectory named *Restore*, which is created in the user or team directory. Users can browse through the files from the disk, copy any needed files, and then delete the *Restore* subdirectory.
4. **System Configuration Restoration** - Restores the system configuration.

idb restoration options

In the Backup Jobs section, icons are displayed to the right of a specific backup in the Action column. These icons enable you to control the way your backups and restored data are handled.

Table 20. idb restoration action icons

| idb restoration action icons | Icon action |
|---|---|
|  | Open Backup: Browses the contents of a specific backup |
|  | Erase Backup: Forcibly deletes any backup (and its children, if any) that is not locked |
|  | Re-Verify Backup: Manually verifies an individual backup |
|  | Lock Backup: Locks an individual backup A locked backup cannot be deleted and idb does not expire this backup |

Table 20. idb restoration action icons (continued)

| | |
|---|---|
|  | <p>Unlock Backup: Unlocks an individual backup if you have a backup that is autolocked because it has a child which is also locked, you must first unlock the child backup</p> |
|---|---|

Locking and unlocking backups

A feature of the idb technology in Lotus Foundations is the ability to lock and unlock individual backups. This enables an administrator to enforce which backups do and do not expire on the idb disk. Backups might also be automatically locked due to the system's autonomies. Locking occurs in the following cases:

- An individual backup has been manually locked by the administrator for preservation.
- A series of backups have been automatically locked as they are parental backups belonging to an incremental backup which has been manually locked.
- A backup which is currently in use is locked automatically for a period of 15 minutes after the task has finished. This occurs during a backup or a restoration procedure.

Initiating a full system idb restoration

A copy of your server configuration is made each time a backup is performed. This configuration file can be used to restore your entire Lotus Foundations server in the event of a catastrophic system failure.

To restore the entire Lotus Foundations system including the server configurations and all of the user data, follow these steps:

1. Click **Backup** in the left side menu of WebConfig. The main idb status page is displayed.
2. Click the Restore from Job icon  in the Action column for the backup job from which you want to restore files. The Restore Files page is displayed, which displays a list of backups and the date and time that the backup was performed.
3. Click the Open Backup icon  in the Action column for the backup from which you want to restore.
4. Click the **Yes** radio button for only the Select All section.
5. Click the **Start Restore** button to begin the restoration procedure. To exit the Restore Files page without completing a backup, click **Close Backup** above the Action column.

Initiating a directory idb restoration

1. Click **Backup** in the left side menu of WebConfig. The main idb status page is displayed.
2. Click the Restore from Job icon  in the Action column for the backup job from which you want to restore files. The Restore Files page is displayed, which displays a list of backups and the date and time that the backup was performed.
3. Click the Open Backup icon  in the Action column for the backup from which you want to restore.

Note: The first entry in the Restore Files section of the page below the Select All option is the System Configuration option. The system configuration is automatically backed up every time any backup is

performed. Restoring system configuration files overwrites the current system configuration, so be very careful with this setting. Leave the default setting, which is **No**.

4. Indicate which directories you want included in the restoration procedure:
 - Select **Yes** if you want the directory restored in normal mode, which overwrites the existing contents of the directories.
 - Select **No** if you do not want this directory restored.
 - Select **Safe** if you want the directory restored in safe mode. This restores files to a *Restore* directory. Selecting all directories is the equivalent of performing a full system restore.
5. Click the **Start Restore** button to begin the restoration procedure.

Initiating a file idb restoration

1. Click **Backup** in the left side menu of WebConfig. The main idb status page is displayed.
2. Click the Restore from Job icon  in the Action column for the backup job from which you want to restore files. The Restore Files page is displayed, which displays a list of backups and the date and time that the backup was performed.
3. Click the Open Backup icon  in the Action column for the backup from which you want to restore.

Note: The first entry in the Restore Files section of the page below the Select All option is the System Configuration option. The system configuration is automatically backed up every time any backup is performed. Restoring system configuration files overwrites the current system configuration, so be very careful with this setting. Leave the default setting, which is **No**.

4. Click the Open icon  in the Action column for the directory that contains the data you want restore.
5. Indicate which file(s) you want included in the restoration procedure.
 - Select **Yes** if you want this file or folder restored in normal mode. The existing data is overwritten.
 - Select **No** if you do not want this file or folder restored.
 - Select **Safe** if you want the files and folders restored in safe mode. The data is saved in the Restore file in each respective user's share. Selecting all files is the equivalent of performing a full directory restore.
6. Click the **Start Restore** button to begin the restoration procedure.

Initiating a restoration from the Lotus Foundations Appliance control panel

This can only be done with a Lotus Foundations Appliance. All other hardware platforms must initiate a restore from the system's WebConfig menu.

Note: Initiate a restoration procedure from the control panel only if you want to perform a complete system restoration.

Press the Restore button. The display panel shows a 10-second countdown, during which time you can stop the restore process by pressing the Cancel button. After 10 seconds, the restore procedure commences and the display panel shows a progress bar.

Lotus Domino restoration procedures

Preliminary Steps

Preliminary Steps

Before restoring your data, consider the following:

1. Decide what data you want to restore. You may want to restore all data, or a specific Domino database or folder. For example, you may only need to restore a particular user's mail file, or perhaps all mail files. The procedures are similar for each case, as you have the option of choosing which folders or databases you want to restore. Note that user mail databases are stored in a folder called mail. A user's mail file has the .nsf extension. For example, if John Doe's username is **jdoe**, his mail file is mail/jdoe.nsf.
2. Decide from where you want to restore the data. The notesbackup team contains the most recent backup, while idb contains older versions. The backup in the notesbackup team is a good place to restore from when a database has been corrupted or data accidentally deleted from it since the last time the Domino backup ran. If you need to go back further in time, you should restore from idb.

Lotus Domino restoration procedures

Restoring idb data from Lotus Domino differs slightly from the standard idb restore process. Follow the instructions carefully to ensure a successful restoration of your Lotus Domino data.

Overview of the Procedure

This is an overview of the procedure. Detailed steps to complete this procedure follow this overview.

1. Stop the Lotus Foundations Start server
2. Locate the desired data to restore. Use the instructions below corresponding to what you want to restore:
 - a. Restoring data from idb
 - b. Restoring data from the notesbackup team
3. Copy the desired data from the backup, and paste it to the correct location. Use the instructions below corresponding to what you want to restore:
 - a. Restoring all data
 - b. Restoring a specific database
 - c. Restoring a specific folder

Note: Steps 3b and/or 3c may be repeated to restore as many databases and folders as required.

4. Ensure correct file ownership.
5. Restart the Lotus Foundations Start server.

Detailed Instructions

Step 1: Stop the Lotus Foundations Start server

1. Click **Add-ons** in the left side menu of WebConfig.
2. Click the Edit icon  in the Actions column for the Lotus Foundations Start server. The Add-on Settings page is displayed.
3. Locate the **Addon Automatic Start** field and select the **Disable** radio button.
4. Click **Save Changes**.

This turns off your Lotus Foundations Start server.

Note: Users cannot access email until the restoration is complete.

Step 2a: Restoring data from idb

1. Click **Backup** in the left side menu of WebConfig.
2. Click the Restore from Job icon  in the Action column, and then click the Open Backup icon  in the Action column for the backup from which you want to restore data.
3. Click the Open icon  for the Team notesbackup directory, then for the Files/ directory, and then for the notesdata/ directory. A directory labeled backup/ is displayed in the list.
4. Select the **Safe** radio button for the backup directory, then click **Start Restore**. The restore time varies, depending on the amount of data that is contained in the folder.
5. From a Windows workstation, click **Start** → **Run**.
6. In the **Open** field, type the following text (where *server_ip* is the IP address of the server):
`\\server_ip\notesbackup\RESTORE\Files\notesdata`
7. You should see a folder named **backup**.

Step 2b: Restoring data from the notesbackup team

1. From a Windows workstation, click **Start** → **Run**.
2. In the **Open** field, type the following text (where *server_ip* is the IP address of the server):
`\\server_ip\notesbackup\notesdata`
3. You should see a folder named **backup**.

Step 3a: Restoring all data

1. Copy the **backup** folder (select the folder, then press Ctrl+C)
2. Navigate to the following location (where *server_ip* is the IP address of the server):
`\\server_ip\notes`
3. Paste the **backup** folder in this location (click a blank area within the destination folder, then press Ctrl+V)
4. Delete the folder labeled **notesdata**
5. Rename the **backup** folder to **notesdata** by right-clicking the **backup** folder, clicking **Rename** from the pop-up menu, then typing notesdata.

Step 3b: Restoring a specific database

1. Navigate to the desired database within the **backup** folder and copy it (select the database, then press Ctrl+C).
2. Navigate to the following location (where *server_ip* is the IP address of the server):
`\\server_ip\notes\notesdata`
3. Navigate to the same folder from which you copied the database. For example, if you copied a database from the **backup\mail** folder, open the **notesdata\mail** folder.
4. If the database you want to restore still exists in the destination, delete it (select the database and press Delete).
5. Paste the database you are restoring in the destination (click a blank area within the destination folder, then press Ctrl+V).

Step 3c: Restoring a specific folder

1. Navigate to the desired folder within the **backup** folder and copy it (select the folder, then press Ctrl+C).
2. Navigate to the following location (where *server_ip* is the IP address of the server):

```
\\server_ip\notes\notesdata
```

3. Navigate to the same folder from which you copied the folder. If you copied the **mail** folder, you are already in the right folder.
4. If the folder you want to restore still exists in the destination, delete it (select the folder and press Delete).
5. Paste the folder you are restoring in the destination (click a blank area within the destination folder, then press Ctrl+V).

Step 4: Ensure correct file ownership

1. Telnet into the Lotus Foundations server and log in as root or an administrative user.
2. Change to the location of the Domino data:

```
cd /home/notes/Files/notesdata
```
3. Change ownership of all files:

```
chown -R notes:notes .
```
4. Exit the Telnet session.

Step 5: Restart the Lotus Foundations Start server

1. Click **Add-ons** in the left side menu of WebConfig.
2. Click the Edit icon  in the Actions column for the Lotus Foundations Start server. The Add-on Settings page is displayed.
3. Locate the **Addon Automatic Start** field and select the **Enable** radio button.
4. Click **Save Changes**.

This restarts your Lotus Foundations Start server.

idb hot swap

Hot swap is only supported on SCSI and specific IDE system configurations. The Lotus Foundations Appliance supports hot swap.

There are four possible hot swap messages that can appear on the display console:

- **idb HotSwap:OK** - Hot swap is supported and the idb disk is inactive, so it can be safely removed and replaced with another idb drive.
- **DON'T REMOVE IDB** - Hot swap is supported, but the disk is currently being used for a backup/restore operation. You must wait until you see the **idb HotSwap:OK** message again before removing the disk.
- **NO BACKUP DISK!** - Lotus Foundations does not detect the presence of an idb disk. You should insert an idb disk and then click the **Update Status** button on the main page of WebConfig in the Disk Status section. The No Backup Disk message also is displayed if the server is set up with all RAID disks and no idb disk(s).
- **CAN'T HOTSWAP** - Hot swap is not supported on your server; therefore, you should never remove the idb disk without powering down the system.

The idb software leaves the idb disk unmounted until it needs to perform a backup or a restore. During this time, if you remove an idb disk from the Lotus Foundations server, the display panel continues to show **idb HotSwap:OK** until one of these events occurs:

- You manually start a backup/restore
- You click the **Update Status** link in WebConfig
- The next scheduled backup begins

After one of the above events occurs, Lotus Foundations detects that there is no idb disk installed and changes the display console message to No Backup Disk!

Swapping idb hard disks (with hot swap)

1. Verify that the display console displays idb HotSwap:OK. idb hot swapping is only available on certain hardware platforms.
2. Remove the idb disk from the server.
3. Insert the new idb disk into the drive.

Lotus Foundations detects the new idb disk during either its next scheduled backup, or if you log in to WebConfig and click the **Update Status** button.

Swapping idb hard disks (without hot swap)

1. Turn off the main power.
2. Remove the disk from the server.
3. Slide the new hard disk into the drive as far as you can, keeping the handle horizontal.
4. Lower the handle and lock the drive in place with the provided hard drive key.
5. Turn the main power back on.
6. Press the power button.

MySQL server

What is the MySQL Server?

MySQL is an advanced database administration tool that can be used to store dynamic Web page data for services such as online catalogs and stores, create accounting databases, and create address books. MySQL is an advanced feature for users that are familiar with databases and SQL (structured query language). For more information, go to <http://www.mysql.com>.

If the MySQL server is enabled, users on the internal network can access personal databases and the databases of any teams to which they belong. User and team databases are automatically created when user and team accounts are set up.

Setting up Windows for MySQL Access

You can use Microsoft Access to access and manage database tables.

1. You first have to download the MySQL ODBC (Open Database Connectivity) connector. You can download this at <http://dev.mysql.com/downloads/connector/>.
2. On the page that is displayed, click the link for the **Connector/ODBC**. Ensure you are downloading the most recent stable release.
3. From the Windows downloads section of the screen that displays, click the download link for Windows or Windows x64.
4. On the screen that is displayed, select the nearest server to download from.
5. In the window that is displayed, select the download location where you want to save the mysql-connector-odbc file. This set of steps assumes that it is saved to the desktop.
6. Double-click the icon on your desktop and click **Run**.
7. The Microsoft ODBC Setup screen is displayed. Click **Continue**.
8. Select MySQL from the Available ODBC Drivers list. Click **OK**.
9. For Windows XP and later, click **Start** → **Settings** → **Control Panel** → **Administrative Tools** → **Data Sources (ODBC)**. For previous versions of Windows, click **Start** → **Settings** → **Control Panel** → **ODBC Data Source**. The ODBC Data Source Administrator screen is displayed.
10. Click **Add...** The Create New Data Source screen is displayed.

11. Select MySQL from the list. Click **Finish**.
12. Provide the following information:
 - a Windows DSN Name (such as MySQL Address Book)
 - your Lotus Foundations server's host name or IP address
 - your MySQL database name, user name, and password.
13. Click **OK** on this screen and then on the ODBC Data Source Administrator screen.
14. Open Microsoft Access.
15. Create a database named address book.
16. Anywhere in this window, right-click your mouse. Select **Link Tables**.
17. In the Files of Type section of the screen that is displayed, select ODBC Databases. The Select Data Source screen is displayed.
18. Select the Machine Data Source tab and select MySQL Address Book. The Link Tables screen is displayed.
19. Select the appropriate table, then click **OK**.
20. Make sure that the appropriate table is highlighted and click **OK**. The table opens in Microsoft Access.

What is a dynamic Web site?

Dynamic Web sites, such as online stores or catalogs, use databases to store information and PHP: Hypertext Preprocessor (PHP) or Perl scripts to produce the Web page based on the data stored in the database. This enables the changing information to be reflected on the site as it changes. Dynamic Web sites require advanced knowledge of PHP or Perl script, and it is advisable that you seek the help of a qualified programmer to create your own.

Generating dynamic Web sites

The following PHP script is used to render the example address book into a dynamic Web site.

1. Ensure you have a team named *AddressBook* on your Lotus Foundations server.
2. Ensure the user *John* is a member of the *AddressBook* team.
3. Enter the following script into a text file and save it as `addressbook.php`:


```
<?php
mysql_connect("localhost", "john", "password");
mysql_select_db("john");
$result = mysql_query("SELECT * FROM AddressBook");
while ($line = mysql_fetch_array($result))
list ($name[],$phone[]) = $line;
for ($i = 0; $i < sizeof($name); $i++)
echo "<tr><td>$name[$i]</td><td>$phone[$i]</td></tr>\n";
?>
```
4. In the Windows Network Neighborhood, copy the script in John's WWW folder on the local server.
5. Open an Web browser on your workstation. In the address bar of the browser, enter:


```
http://server_name/~john/addressbook.php
```

The address book opens in the browser.

Hardware components reporting

Lotus Foundations has the capability to report on hardware that is detected in the server—including processors, memory, Ethernet and hard drives—and verify whether or not that hardware is currently supported by the version of Lotus Foundations running.

The **Hardware Status** page displays the details of all the hardware on the system, and information pertaining to the compatibility/support of the hardware within the current version of Lotus Foundations.

To view the Hardware Status list, click **Hardware Status** in the left side menu of WebConfig. The Hardware Status page is displayed.

While the server polls the hardware, the Hardware Status page displays the following message: (Collecting hardware status data. Please wait...)

The information displayed varies according to the specific hardware in your server.

Table 21. Hardware Status columns

| Column | Description |
|-------------|---|
| Type | Type of hardware being reported; for example, CPU and memory |
| Description | Brand of hardware |
| Device ID | Where the hardware is located in the server |
| Status | Specifies if the hardware is one of three states: <ul style="list-style-type: none">• Supported - Has its required drivers installed in the Lotus Foundations operating system• Unsupported - Does not have its driver installed• Support Unknown - The Lotus Foundations operating system cannot determine the required driver |

Log messages

Accessing log messages

Lotus Foundations keeps a log that displays the messages from all of the Lotus Foundations subsystems. To view the log from the firewall subsystem, please refer to the “*Firewall log*” section.

To access this log click **Logs and Reports** in the left side menu of WebConfig. The Log Messages page is displayed.

Customizing message display

The **Highlight** drop-down menu enables you to highlight messages coming from a specific Lotus Foundations subsystem, such as Disk manager and Fast/Port Forward, making them easier to view.

To customize your message log display follow these steps:

1. Select a subsystem from the **Highlight** drop-down menu.
2. Select an option from the **Priority** drop-down menu.
 - The priority list customizes what kind of message is highlighted.
 - By default, only messages that show a change in the system display; however, you can display error messages and debug messages.
3. Click **Apply**. The appropriate messages are highlighted.

Firewall log

For ICSA Labs firewall compliance, Lotus Foundations logs requests to send traffic through the firewall. See the “*Firewall services*” on page 99 chapter for more information on the Lotus Foundations firewall. Firewall logging is only enabled when the **Restrict Outgoing Connections** field is set to **Yes**.

The following firewall information is logged:

- All permitted inbound access requests from public network clients that use a service identified in the security policy hosted on the Lotus Foundations server itself or on a private or service network server.
- All permitted outbound access requests from private and service network clients that use a service identified in the security policy on a public network server.
- All access requests from private, service, and public network clients to traverse the Lotus Foundations firewall that violate the security policy.
- All access requests from private, service, and public network clients to send traffic to the Lotus Foundations server itself that violate the security policy.
- All attempts to authenticate at an Administrative Interface on the Lotus Foundations server itself.
- All access requests from private, service, and public network clients to send traffic to the Lotus Foundations server itself on the port or ports used for Remote Administration.
- Each Startup.

The logs contain the following information:

- **Date and Time:** When the event occurred with an accurate datestamp and timestamp
- **Protocol:** TCP, UDP, ICMP, Other
- **Source IP Address**
- **Destination IP Address**
- **Destination Port:** Either TCP and UDP or Message Type; for example, ICMP
- **Disposition of the event:** For example, Blocked or Allowed

To view the firewall log, you must be a member of the *log* team. This team is automatically created by Lotus Foundations.

The firewall log file is displayed in the team folder on Lotus Foundations. The file `wvlog.current` contains the latest log messages.

To add a user to the *log* team, follow these steps:

1. Click **Users** in the left side menu of WebConfig. The **Users** tab of the User Setup page is displayed.
2. Click the appropriate user's edit icon  in the Action column. The Modify User screen is displayed.
3. Select the *log* team in the **Join Teams** field. Click **Join** . The team is displayed in the Member of Teams field.
4. Click **Save Changes**.

Network file system

What is NFS?

NFS (Network File System) is a protocol invented by Sun Microsystems that enables clients using UNIX and similar operating systems to mount file systems from remote servers. This chapter is for advanced users who are familiar with UNIX and similar operating systems. Refer to <http://en.tldp.org/HOWTO/NFS-HOWTO/> for more information on NFS.

Lotus Foundations only supports situations where the user IDs are the same on the local system and the Lotus Foundations server.

rsync

What is rsync?

rsync is a UNIX-based utility that enables incremental files and directory synchronization from one location to another. This can be used to copy data files from the Lotus Foundations server to another system that also supports rsync. An advantage to using this file transfer method is that only the changed portions of the files are transferred, rather than the entire new version of the files and directories.

Note: To use rsync, commands must be run within a Telnet session. Therefore, basic knowledge and understanding of the Linux command line is strongly recommended. For a more detailed explanation of rsync, please visit the following Web site: <http://samba.anu.edu.au/rsync/>

Enabling rsync

To enable rsync, follow these steps:

1. Log into WebConfig as an administrative user.
2. Click **Local Network** in the left side menu of WebConfig. The **Basic Setup** tab of the Local Network Setup page is displayed.

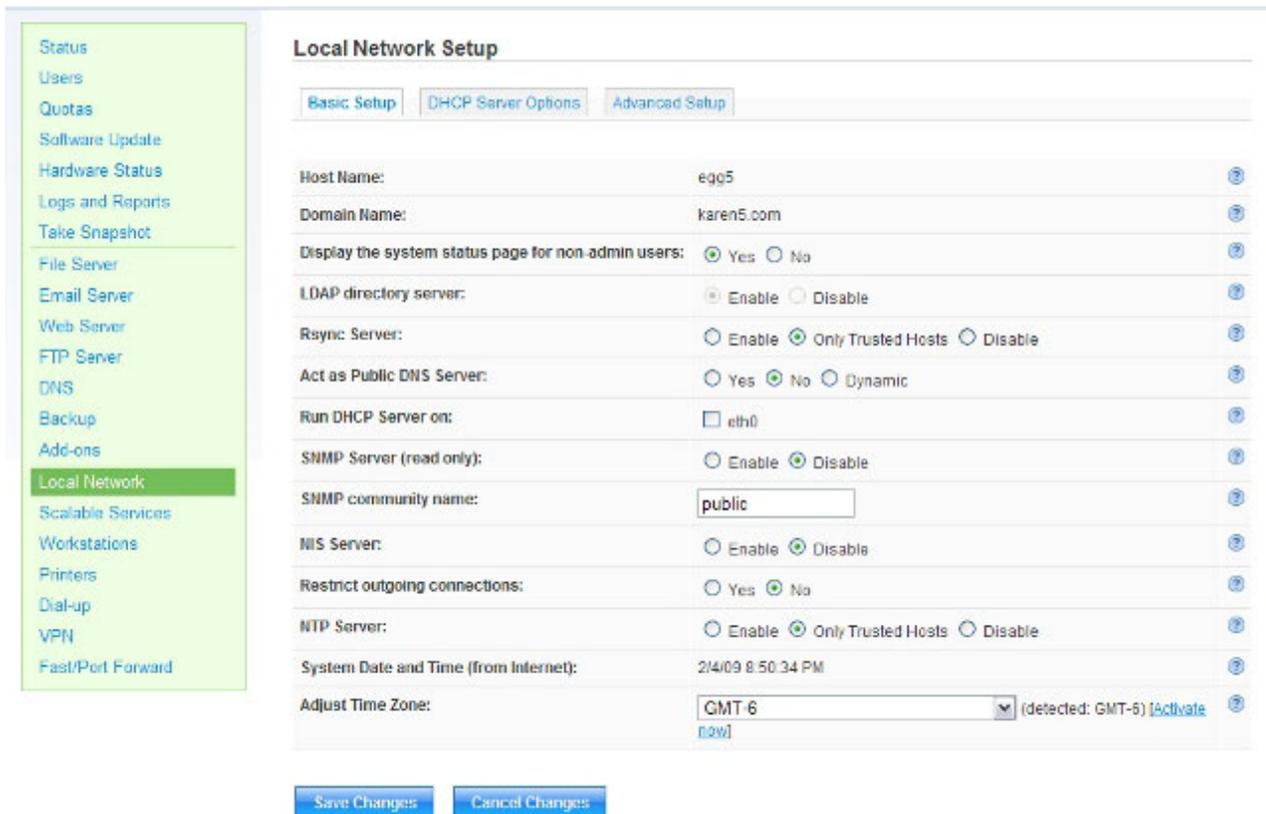


Figure 48. Basic Setup tab of the Local Network Setup page of WebConfig

3. For the **Rsync Server** field, select **Enable** or **Only Trusted Hosts**.
4. Click **Save Changes**.

rsync from a Telnet session

Pushing data to another location

To push data to another location, use this command:

```
rsync -zav --progress /home/local_user/Files remote_user@remote_server::remote/path/
```

Table 22. Options for the rsync push command

| Command option | Explanation |
|---------------------------|---|
| rsync | rsync executable command |
| -z | Compresses any data from the files rsync sends to the destination computer (useful for slow connections); the compression method is the same method used by the UNIX gzip compression utility |
| -a | Enables recursion and preserves almost everything during the synchronization |
| -v | Increases the amount of information you receive during the transfer (default is for rsync to work silently); a single -v provides information about which files are transferring and a brief summary at the end, while two -v flags provides information about skipped files and slightly more information at the end |
| --progress | Displays the progress of individual files |
| /home/local_user/* | Local directory to push out to the remote location |
| remote_user@remote_server | remote_user is the team name at the remote location and remote_server can be either the remote server's IP address or the fully qualified domain name; the password prompt following the rsync line is for this account |
| :: | A double colon in the destination field copies from the local server to the remote server; a double colon also separates the host name from the path that follows |
| remote/path | Destination folder or path |
| / | Eliminates confusion rsync might have with the command when appended to the trailing directory; without it, the path might be interpreted as /REMOTE_USER/dir/dir/ or something similar |

You are then prompted to provide the password for the *remote_user* account entered into the syntax.

Pulling data from another location

To pull data from another location, use this command:

```
rsync -zav --progress remote_admin@remote_server::remote_user/* /home/local_user/Files
```

- The transfer is initiated by the local server, but the files are pulled from the remote server.
- The double colon indicates from where the files are copied.
- /home/local_user/Files represents the path to the destination folder on the local system.

As with the push method, you are prompted to provide a password for the *remote_admin* account.

Lotus Foundations Run feature

The Lotus Foundations Run feature provides users with the ability to run Windows applications on a Lotus Foundations server. This can be important when you find that you want to use the functions of idb and the ease of user management, but the client has an application that has to run on a Windows operating system. To accomplish this, a VMware server runs in an NVS environment. The user interface within the Webconfig console provides the ability to control the virtual server and customize

configuration and backup settings. Additionally, if you have pre-built VMware images in a zip file format, Lotus Foundations Run can automatically import them into the VMware server.

What is VMware?

VMware is the virtualization platform used by the Lotus Foundations Run add-on. Virtualization allows users to transform or "virtualize" the hardware resources of a computer, including the CPU, memory, hard disk and network controller, to create a fully functional virtual machine that can run its own operating system and applications. Multiple virtual machines share hardware resources without interfering with each other, so users can run several operating systems and applications at the same time. Software virtual appliances are pre-built software, comprised of one or more virtual machines that are packaged, updated, maintained and managed as a unit. You can easily install and deploy these pre-integrated solution stacks. For more information on VMware and its capabilities, go to <http://www.vmware.com/>.

Installing the Lotus Foundations Run 1.1 add-on

Note: For the Lotus Foundations Run add-on, Lotus Foundations Start must be installed on a hardware platform and not as a virtual machine itself. VMware Server 2 for Linux does not work on a virtual installation of Lotus Foundations Start.

The Lotus Foundations Run add-on installation is done in two parts:

- Lotus Foundations Run installation
- VMware Server 2 add-on for IBM Lotus Foundations Run 1.1 installation

Prerequisites

Before you begin installing the Lotus Foundations Run add-on onto a Lotus Foundations server, ensure you have:

- 2 GB of physical memory (in addition to what is required for Lotus Foundations Start)
- A license key from VMware for VMware Server version 2 for Linux. See "Obtaining a license key for VMware Server 2 for Linux" for information on how to obtain a free license key for VMware Server 2 for Linux.
- Lotus Foundations Run installation package
- VMware Server 2 add-on for IBM Lotus Foundations Run 1.1 installation package located at http://www.ibm.com/services/forms/preLogin.do?lang=en_US&source=swg-vmwares2a
- One of the following Web browsers on a client workstation with access to the Lotus Foundations Start server:
 - Mozilla Firefox 2.0 or 3.0 for Linux
 - Mozilla Firefox 2.0 or 3.0 for Windows
 - Internet Explorer 6.0 SP1 or 7.0
- *Optional:* Pre-built VMware images

Obtaining a license key for VMware Server 2 for Linux

If you do not already have a license for VMware Server 2 for Linux, you can obtain one online for free by following these steps:

1. Proceed to the VMware free virtual server registration page (<http://www.vmware.com/freedownload/login.php?product=server20>).
2. On the registration web page, enter your first name, last name, and email address. A valid email address must be provided in order to send the license information. Click **Continue**.

3. On the following page, provide information about your company and your usage for VMware. You must also agree to the license terms and agreements. When asked "How many Hosts will have VMware installed?", make sure you enter at least one (1) for Linux.
4. Click the **Register** button to complete the registration process.
5. Two emails containing the registration information and the activation link are sent to you immediately. Upon receiving the activation email, open the message and click **Activate Now**.
6. A web browser window opens and takes you to a page where you are required to enter your email address along with the password you provided during the registration process.
7. Upon authentication, you are provided the license information for VMware Server 2 for Linux. Save this license key as you need it later to complete the Lotus Foundations Run setup with VMware.

Lotus Foundations Run installation

Before installing VMware Server 2 add-on for IBM Lotus Foundations Run 1.1, you must first install Lotus Foundations Run. With the Lotus Foundations server running and configured, follow these steps:

1. *Optional:* If you have any pre-built VMware images in a ZIP file format, follow these steps:
 - a. Connect to the **autoinstall** folder on the Lotus Foundations server. To do this, from a workstation, click **Start** → **Run** and then enter '\\\' followed by the server's IP address, followed by \autoinstall. For example, \\192.168.0.1\autoinstall.
 - b. Create a folder titled **vmdir**.
 - c. Place the pre-built image ZIP files in the \\server_ip_address\autoinstall\vmdir directory.

Note: For any pre-built VMware images in a ZIP file format placed in this directory after the installation of Lotus Foundations Run, the add-on needs to be restarted for the VMware server to import them.
2. If you have a DVD, insert the DVD labeled **Lotus Foundations Start, Disk 2** into the server. If you downloaded the software to your workstation, do the following:
 - a. Connect to the **autoinstall** folder on the Lotus Foundations server. To do this, from a workstation, click **Start** → **Run** and then enter '\\\' followed by the server's IP address, followed by \autoinstall. For example, \\192.168.0.1\autoinstall.
 - b. Enter the administrative account and password.
 - c. Locate the folder where you unzipped the Lotus Foundations Run add-on package. The naming convention is lf-run11-*nnnn*.pkg (for example, lf-run11-5256.pkg).
 - d. Place the lf-run11-*nnnn*.pkg into the **autoinstall** folder. Wait to proceed until all of the files are copied to the server **autoinstall** directory.
3. Login to the Webconfig console and click **Software Update** from the menu on the left side.
4. In the "Add-on packages available for install" section, you should see an option for the Lotus Foundations Run add-on. Click the corresponding **Install** link.
5. Read and accept the license agreements and the installation process begins.
6. Verify the setup is complete on the main status page in the **Add-ons** section. Until you install the VMWare Server 2.0, the status on the **Add-ons** screen displays as 'inactive.'

VMware Server 2 add-on for IBM Lotus Foundations Run 1.1 installation

Follow these steps to install the VMWare Server 2.0 for Lotus Foundations Run onto Lotus Foundations Start:

1. If you burned this CD, insert the CD into the server (see "Prerequisites" on page 133 for the installation package location).
If you downloaded the software to your workstation, do the following:

- a. Connect to the **autoinstall** folder on the Lotus Foundations server. To do this, from a workstation, click **Start** → **Run** and then enter '\\\' followed by the server's IP address, followed by \autoinstall. For example, \\192.168.0.1\autoinstall.
 - b. Enter the administrative account and password.
 - c. Locate the folder where you unzipped the VMWare Server 2.0 for Lotus Foundations Run package. The naming convention is lfrun-vmware20-*nnnn*.pkg (for example, lfrun-vmware20-5256.pkg).
 - d. Place the lfrun-vmware20-*nnnn*.pkg into the **autoinstall** folder. Wait to proceed until all of the files are copied to the server **autoinstall** directory.
2. Login to the Webconfig console and click **Software Update** from the menu on the left side.
 3. In the "Add-on packages available for install" section, you should see an option for the VMWare Server 2.0 for Lotus Foundations Run. Click the corresponding **Install** link.
 4. Read and accept the license agreements.
 5. In the **Input Serial Number** field, enter the serial number you received in "Obtaining a license key for VMware Server 2 for Linux" on page 133 and click **Submit**. The installation process begins.
 6. Verify the setup is complete on the main status page in the **Add-ons** section.

Using the VMware server

After you have successfully installed the Lotus Foundations Run add-on, you can access the VMware server administration console two ways:

- Open a web browser and connect to the following URL:
http://*server_ip_address*:8222
- In the Webconfig console, click **Add-ons** from the left side menu. Select the **Virtualization** tab and click **Advanced Virtualization Settings**.

If you copied any pre-built ZIP file VMware images over before the installation of the Lotus Foundations Run add-on (as shown in "Lotus Foundations Run installation" on page 134), they have been automatically unzipped and placed in the correct directory.

Adding a pre-built VMware image folder

If you want to add pre-built VMware image folders, follow these steps:

1. Copy the entire folder to the following location on the Lotus Foundations server:
server_ip_address\lf-virtualization\filesystem\var\lib\vmware\Virtual Machines
2. Access the VMware administration console and select **Add Virtual Machine to inventory**. In the **Add Existing Virtual Machine** dialog, select your image and click **OK**. You are ready to use your VMware image.



Figure 49. Adding a virtual machine to inventory

Using the VMware administration console, you can change the size of the virtual disk, the amount of memory, configure connections, and set permissions. Refer to the VMware Server 2.0 documentation (http://www.vmware.com/support/pubs/server_pubs.html) for general how-to documentation and step-by-step instructions on using VMware.

VMware configuration tips

- If you are using VMware in a heavy input/output (IO) environment, there are some configurations you can make to optimize performance, such as:
 - Adding more physical memory
 - Configuring the VMware hard disk as pre-allocated disk space
 - Increasing the memory for the guest operating system
- When adding VMware ISO images, the ISO must be copied in to a NSF file system (file share) on the Lotus Foundations server. If you want to point a datastore at an NFS file, you first need to ensure the NFS file server is enabled on the Lotus Foundations server. To do this, click **File Server** in the left side menu in the Webconfig console. In the **NFS file server** row, click the **Enable** radio button. Click **Save Changes**.

Additional VMware resources

The following additional VMware resources can be useful with Lotus Foundations Start:

- **The vCenter Converter:** The vCenter Converter takes a snapshot of a physical machine and creates a VMware virtual machine image. This can assist you in replicating a production environment into a test environment. For more information, go to <http://www.vmware.com/download/converter/>.
- **VMware Ready program:** The VMware Ready program lets a customer know your application/solution has met a specific set of VMware-specified integration or interoperability criteria and is ready for optimal use with other VMware data centers or desktop solutions. For more information, go to <http://www.vmware.com/partners/vmware-ready/index.html>.

Editing Lotus Foundation Run add-on settings

You can edit some of the Lotus Foundations Run add-on settings by following these steps:

1. In the WebConfig console, click **Add-ons** in the left-side menu of WebConfig.
2. The **Status** tab is the default view. Click the edit icon  for Lotus Foundations Run.
3. *Optional:* Edit the **Start Command** field to change the name of the program that you want to use to start up the add-on. It must be placed in the directory of the user who shares a name with this add-on.
Note: It is recommended you do not change this setting. If modified incorrectly, the add-on does not function properly.
4. *Optional:* Edit the **Monitor Command** field to change the name of the program that monitors the health of the add-on. It must be placed in the directory of the user who shares a name with this add-on and must publish its information into the `/tmp/addons/addon-name/status` section of the `uniconf` tree.
Note: It is recommended you do not change this setting. If modified incorrectly, the add-on does not function properly.
5. *Optional:* Edit the **Firewall Port(s)** field if you need to list ports to open up on the untrusted interfaces and allow external users to connect to programs running in the add-on. The ports in the list must be separated by spaces. By default this field is blank.
6. *Optional:* The **Addon Automatic Start** option lets you select whether or not you want Lotus Foundations to start the add-on automatically on startup. The default is set to **Enable**.

Virtualization tab

The **Virtualization** tab helps you access and start or stop your virtual applications. The figure and table below illustrate the different options for each virtual application.

Add-ons

Status **Virtualization**

| Status | Datastore | Application Name | Disk Space Used | Memory Size | IP | Backup | Action |
|---|-----------|--|--|-------------|----|-------------------------------------|---|
|  | standard | Windows 2003 Server R2 with Dsktop Apps Loaded and MS Licenses Activated | 0 bytes Used 0 bytes Total (0% Used) | 384.0 MB | -- | <input checked="" type="checkbox"/> |   |

Figure 50. Virtualization tab

Table 23. Virtualization Tab

| Item | Description |
|----------------------------------|--|
| Status |  - The virtual machine is running.  - The virtual machine is stopped. |
| Datastore | The directory where VMware keeps virtual machine files/configuration. VMware Server 2.0 supports multiple stores and each store has a unique name. The default store is Standard . |
| Application Name | The name of the virtual application. |
| Disk Space Used | The amount of disk space used and the total amount of disk space available. |
| Memory Size | The amount of memory is being used or will be used by the image. |
| IP | The IP address of the virtual machine. To display the IP address, a user needs to install VMware tools inside of guest operating system. By default, this is blank. |
| Backup | Option to select to back up or not back up the virtual machine as part of the LF Virtualization Backup job. See "Backup & Restore" on page 114 for details. The default is set to back up. Remember to select Save Changes if you change the default. |
| Action | Start or stop your virtual machine. |
| Advanced Virtualization Settings | Opens the VMware server administration console (http://server_ip_address:8222). |

Restarting the Lotus Foundations Run add-on

You might need to restart the VMware server if it stops responding or you added a VMware image in a ZIP file format that you want automatically imported. To restart the VMware server, follow these steps:

1. Login to the Webconfig console and select **Add-ons** from the left-side menu.
2. Click the edit icon  for the Lotus Foundations Application Engine. Next to **Addon Automatic Start**, click **Disable**. Click **Save Changes**.
3. Wait approximately 30 seconds, click the edit icon again, and then click **Enable** for **Addon Automatic Start**. Click **Save Changes**.

Backing up and restoring the virtual machine

When you install the Lotus Foundations Run add-on, a backup job called **LF Virtualization Backup** is created. You can select which virtual applications you want to be backed up through the “Virtualization tab” on page 137 in the WebConfig console. When you select to have a virtual application backed up, the entire VMware image is backed up. This includes configuration and virtual disk files for the guest operating system. When selected, the VMware image is backed up every day at 1:00 AM.

If you cannot back up all VMware images, it is recommended that at a minimum the guest operating system files are backed up. For Windows, an administrator should be familiar with how to use Windows shares with Lotus Foundations. Map a shared team directory in Windows and store the data in this directory. On the Lotus Foundations server, the administrator needs to make sure that the shared team directory is backed up by the Master Job or another idb backup job.

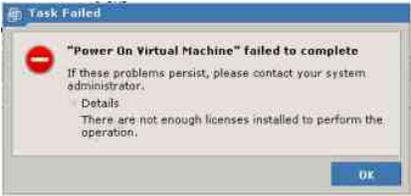
The frequency of when the backup occurs can be changed, along with other options, by clicking **Backup** from the left side menu in the WebConfig console and clicking on the job name. For more information on using the backup and restore options, see “Backup & Restore” on page 114.

Troubleshooting

Table 24. Troubleshooting Tips

| Error or Warning | Possible Cause | Possible Solution |
|--|--|--|
| <p>Error: \\server_ip_address\lf-virtualization The network path was not found</p>  <p>This error occurs when trying to map to lf-virtualization folder on the Lotus Foundations Start server from a workstation.</p> | <p>Lotus Foundations Run add-on (lf-run11-<i>nnnn</i>.pkg) is not installed.</p> | <p>Install the Lotus Foundations Run add-on (lf-run11-<i>nnnn</i>.pkg).</p> |
| <p>Warning: Lotus Foundations Application Engine: Application components are not correctly installed.</p>  <p>This warning occurs in the WebConfig status page for Add-ons after the Lotus Foundations Run add-on (lf-run11-<i>nnnn</i>.pkg) is installed but VMWare Server 2.0 for Lotus Foundations Run (lfrun-vmware20-<i>nnnn</i>.pkg) is not yet installed.</p> | <p>The Lotus Foundations Run add-on (lf-run11-<i>nnnn</i>.pkg) is installed but VMWare Server 2.0 for Lotus Foundations Run (lfrun-vmware20-<i>nnnn</i>.pkg) is not yet installed.</p> | <p>Install the VMWare Server 2.0 for Lotus Foundations Run (lfrun-vmware20-<i>nnnn</i>.pkg).</p> |

Table 24. Troubleshooting Tips (continued)

| Error or Warning | Possible Cause | Possible Solution |
|---|---|---|
| <p>Error:</p>  <p>This error occurs when an invalid VMware license was used in the installation of the VMware 2.0 Server for Lotus Foundations Run package.</p> | <p>An invalid VMware license was used in the installation of the VMware 2.0 Server for Lotus Foundations Run package.</p> | <p>Uninstall the Lotus Foundations Run add-on and reinstall using a valid license number.</p> |

Lotus Symphony

Lotus Symphony is a product suite that contains the following productivity tools:

- A word processor
- A presentation editor
- A spreadsheet editor

Lotus Symphony is available as both a stand-alone offering and as an embedded client that can run in the Lotus Notes 8.0x client.

Lotus Symphony tools support the Open Document Format (ODF), which ensures the ability to access, use, and maintain documents without concern for end of life, or ongoing software licensing and royalty fees. Using the productivity tools that collectively compose Lotus Symphony, end users can create, manage, edit, and import documents in ODF. The Lotus Symphony tools can also import, edit, and save documents in Microsoft Office formats or export those documents to ODF for sharing with other applications.

How does Symphony compare to other similar offerings?

Lotus productivity tools provide an alternative for users who perform basic to moderately complex document tasks. The following list illustrates the similar offerings that Lotus Symphony can provide an alternative solution for:

- Lotus Symphony supports Microsoft Office 97/XP/2000/2003 formats.
- Lotus Symphony can open documents, spreadsheets, and presentations created by Lotus SmartSuite®. The files can be saved in any of the file formats supported by Symphony.
- Lotus Symphony can open, edit, and save, OpenOffice files.

More information about Lotus Symphony

To learn more about using Lotus Symphony or for product support, refer to the Lotus Symphony website at the following URL:

<http://symphony.lotus.com/software/lotus/symphony/>

Installing Lotus Symphony add-on to the server

The first part of the installation of Lotus Symphony installs the server add-on package on the Lotus Foundations server. To install the server add-on package to the Lotus Foundations server, with the Lotus Foundations server running and configured, follow these steps:

1. If you have a DVD, insert the DVD labeled **Lotus Foundations Start, Disk 2** add-on into the server. If you downloaded the software to your workstation, do the following:
 - Connect to the **autoinstall** file share on the Lotus Foundations server. To do this, from the workstation, click **Start** → **Run**, and then enter '\\\' followed by the server's IP address, followed by \autoinstall. For example, \\192.168.0.1\autoinstall.
 - Enter the administrative account and password.
 - Locate the folder where you unzipped the Lotus Foundations Start Symphony package. The naming convention is lf-symphony12-*nnnn*.pkg. (for example, lf-symphony12-2760.pkg)
 - Place the Lotus Symphony lf-symphony12-*nnnn*.pkg into the **autoinstall** folder. Wait to proceed until all of the files are copied to the server **autoinstall** folder.
2. Select **Software Update** from the menu on the left side of the WebConfig screen.
3. A list of installable packages is displayed. If there is no list of available packages, wait several seconds and refresh the screen again. The Lotus Symphony add-on package should be listed and should be displayed as: Lotus Symphony 1.2 (Team autoinstall/lf-symphony12-*nnnn*.pkg).
4. Click **Install** on the Lotus Foundations Start Lotus Symphony add-on; read and accept the license agreements. The installation begins immediately and might take a few moments.
5. Verify the setup is complete on the main status page in the Add-ons section.

The Lotus Symphony package that is deployed to the Lotus Foundations server includes support for all languages.

Installing Lotus Symphony to client workstations

Client requirements

The following list contains the client system requirements:

- Supported Windows platforms: Windows XP + SP2, Windows Vista
- At least 750MB of free disk space on Linux and at least 540MB of free disk space on Windows
- At least 512MB RAM memory

Windows installer does not support AMD64 CPU with XP/Vista 64 bit platforms installed.

Prerequisite

You must uninstall any previous versions of Lotus Symphony before installing the version integrated with Lotus Foundations.

Uninstall previous versions of IBM Lotus Symphony on Windows

Follow these steps to uninstall any previous versions of Lotus Symphony:

1. Close IBM Lotus Symphony before uninstalling.
2. Open the Control Panel by clicking **Start** → **Control Panel**.
3. Double-click **Add or Remove programs**.
4. Select IBM Lotus Symphony, and click **Remove**.

Installing IBM Lotus Symphony on Windows XP and Windows Vista

Follow these steps to install Lotus Symphony to the client workstation:

1. *Optional:* Specify the local language setting on the user's workstation. Click **Start** → **Control Panel** → **Region and Language Options**, if necessary. Lotus Symphony version 1.2 automatically switches to the native language version specified in this setting.

- From the user's workstation, connect to the user's file share on the Lotus Foundations server. To do this, click **Start** → **Run**, and then enter '\\\' followed by the server's IP address, followed by \USERNAME. For example, type \\192.168.0.1\USERNAME where USERNAME corresponds to the user that is installing Lotus Symphony.
- Navigate to the **LotusFoundations** → **SYMPHONY1_INSTALL** folder and double-click the SYMPHONY1_SETUP.BAT file, then select **Run** when prompted.

The Symphony Installation and Setup screen displays. Press any key to continue.

Note: When the command prompt window opens, a message is displayed that states: UNC paths are not supported. Defaulting to Windows directory. (as shown in the following screen shot). This message can be ignored.

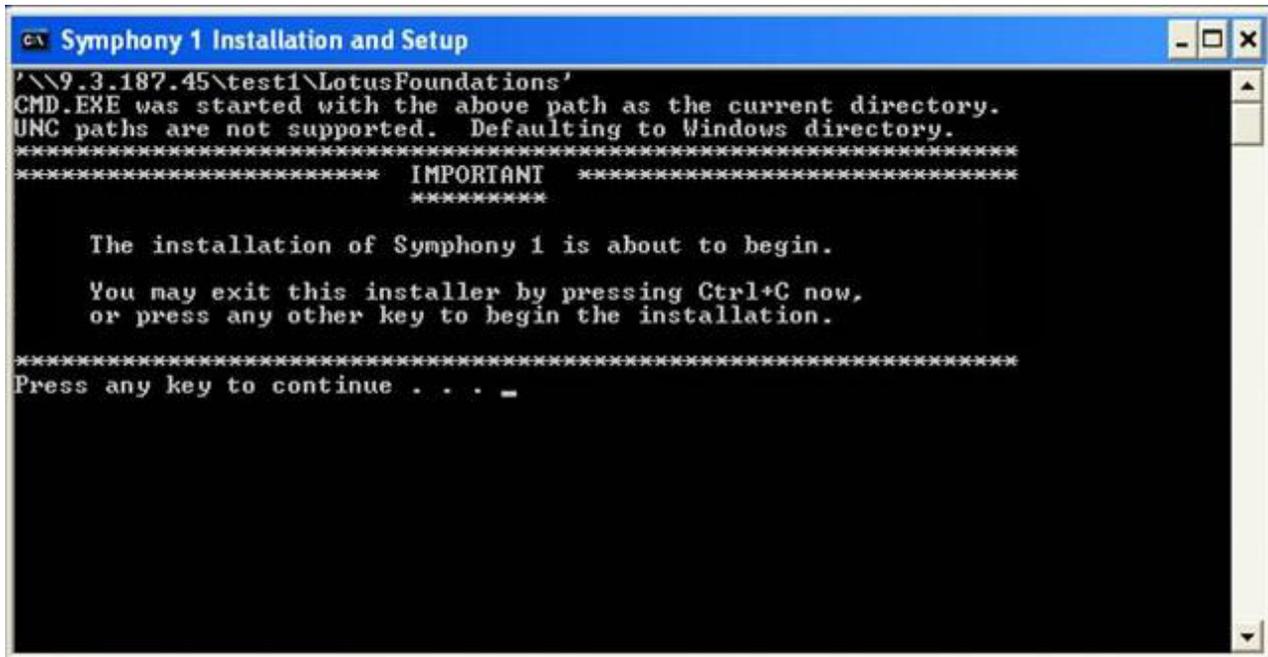


Figure 51. Symphony Installation and Setup screen

- The installation should take approximately five to ten minutes for a workstation that is on the same local network as the Lotus Foundations server. When the installation has completed, a message stating that "Symphony 1 auto setup is configured...Press any key to continue...". Press any key and the program closes.

You are ready to begin working with IBM Lotus Symphony to create new documents, spreadsheets, and presentations. You have one icon for Lotus Symphony on your desktop and one shortcut on the **Start** → **All Programs** menu.

Note: The Lotus Symphony package that is installed from the Lotus Foundations server includes support for all languages and uses the language of the user's workstation.

Switching between languages

You can switch between English and any other supported language by switching system locale on your workstation. IBM Lotus Symphony only supports switching from one non-English language to another language within the same group or to English:

- Group 1 refers to Simplified Chinese, Traditional Chinese, French, German, Italian, Japanese, Korean, Portuguese (Brazilian), and Spanish.

- Group 2 refers to Arabic, Czech, Danish, Dutch, Finnish, Greek, Hebrew, Hungarian, Norwegian, Polish, Portuguese, Russian, Swedish, and Turkish.
- Group 3 refers to Catalan, Thai, Slovak, Slovenian.

Without a successful switch between languages, you might get a partially translated or completely English user interface.

Spam scanner

The spam scanner is an add-on software module. You must have a valid Spam Scanner license to use this feature.

The spam scanner filters all incoming emails received through the Simple Mail Transfer Protocol (SMTP) before the messages are delivered to the user's mailbox. Once filtered, incoming emails are categorized into one of the following three categories:

- Not Spam: Identified as not being spam; sent to the recipient
- Probably Spam: Identified as probably spam; sent to the recipient with the subject header flagged as [Spam?]
- Definitely Spam: Identified as definitely spam; sent to recipient with the subject header flagged as ***SPAM***

Depending on the rules set by each user, the spam scanner does the following with a spam message:

- Do nothing: Sends email to the recipient normally with no modifications
- Mark: Sends email to the recipient with the subject header flagged as ***SPAM*** or [Spam?]

Note: This is the default setting.

- Move to Spam folder: Flags subject header as ***SPAM*** or [Spam?] and moves message to the *Spam* mail directory
- Delete: Deletes message without ever sending to the recipient

To set up rules, see *"Configuring users' spam filters"* on page 143 later in this chapter.

Installing the Lotus Foundations anti-spam network filtering feature

The Lotus Foundations network layer spam scanner is an available feature to any server with an up-to-date spam scanning license. While the content layer spam scanner is installed automatically, the network layer scanner is a separately installed add-on.

To install the Lotus Foundations anti-spam network filtering feature, follow these steps with the Lotus Foundations server running and configured:

1. If you have a DVD, insert the DVD labeled Lotus Foundations Start, Disk #2 into the server.
2. If you downloaded the software to your workstation, follow these steps:
 - a. Connect to the autoinstall file share on the Lotus Foundations server. To do this, click **Start** → **Run**, and then enter the server's IP address followed by \autoinstall. For example, \\192.168.0.1\autoinstall.
 - b. Observe the dialog box and enter the administrative account and password.
 - c. Locate the folder where you unzipped the Lotus Foundations packages. The naming convention is lf-antispam-*nnnn*.pkg (example: lf-antispam-2760.pkg).
 - d. Drag the add-on folder lf-antispam-*nnnn*.pkg into the autoinstall folder. Wait to proceed until all of the files are copied to the server autoinstall directory.
3. Click **Software Update** in the left side menu of WebConfig. A list of installable packages is displayed. If there is no list of available packages, wait several seconds and refresh the screen again. The Lotus

Foundations Anti-Spam add-on package should be listed and should be displayed as Engate Mail Sentinel (Team autoinstall/1f-antispam-nnnn.pkg)

4. Click **Install** on the Engate Mail Sentinel add-on, read the license agreements, and accept the agreements to continue. The installation begins immediately, and might take a few moments to complete.
5. Verify the setup is complete on the Services Status section of the Status page.

On first installation, the network layer spam scanner takes between 6-12 hours to complete the registration process. All updates to the spam scanner, after this initial process, are immediate. You can reduce the time this process needs by occasionally clicking **Check for New Versions** on the Software Update page. Occasionally checking for new versions of software can reduce the time required for this process up to approximately an hour. During this period, the network layer filter is not applied. All mail is still accepted and processed by the content layer spam scanner.

You can reduce the time this process needs by occasionally clicking **Check for New Versions** on the Software Update page.

Engate Mail Sentinel is a trademark of Engate Corporation.

Activating your spam scanner

1. Click **Email Server** in the left side menu of WebConfig. The **Summary** tab of the Email Server Setup page is displayed.
2. Click the **Filters** tab.
3. Select **Enable** in the Mail Spam Scanner field.
4. Click **Save Changes**.

Configuring users' spam filters

1. Click **Users** in the left side menu of WebConfig. The User Setup page is displayed.

| Local | User ID | Full Name | Teams | PPTP | FTP | Email Space Used | Disk Space Used | Action |
|-------|---------|-----------|------------|------|-----|------------------|-----------------|--------|
| | * | test1 | Tester One | | * | 10.0 MB | 124 kB Used | |
| | * | test2 | Test User2 | | * | 9.7 MB | 124 kB Used | |

Figure 52. The Users tab in the User Setup page of WebConfig

2. Click the edit icon  in the Action column for the user you need to edit. The Modify User page is displayed.
3. Click the **User Email Settings** button. The Email Server page is displayed.
4. For the **Treatment of definite spam** and **Treatment of probably spam** fields, select one of the following options:
 - **Do Nothing**
 - **Mark subject**
 - **Move to Spam folder**
 - **Delete**
5. Click **Save Changes**.

Users can change their own treatment of spam by logging into the WebConfig with their user account and changing the setting shown above.

Virus scanner

AntiVirus for Lotus Foundations is an add-on software module. You must have a valid AntiVirus for Lotus Foundations virus scanner license to use this feature. The anti-virus software in Lotus Foundations is provided by Kaspersky, a company that supplies original equipment manufacturers (OEMs) with anti-virus solutions. They have won numerous awards for their anti-virus technology. You can find out more about this company and their award-winning anti-virus technology on the Kaspersky website, located at the <http://www.kaspersky.com/>.

AntiVirus for Lotus Foundations virus scanner gives you complete anti-viral protection for your Lotus Foundations server with both file- and mail-level virus scanning. AntiVirus for Lotus Foundations scans for viruses on the local file system as well as incoming and outgoing email messages including mail collected from external mailboxes. AntiVirus for Lotus Foundations detects infected, suspicious, corrupted and password-protected files, and files that fail to be scanned because of an error. All infected, suspicious and corrupted objects that can not be automatically repaired are quarantined.

File virus scanner

AntiVirus for Lotus Foundations file virus scanner is not a real-time scanner, meaning that it does not scan for viruses as data is transmitted, copied, or moved to the Lotus Foundations server. Instead, the Lotus Foundations server runs a scheduled file scan once every 12 hours by default. This provides maximum stability and available resources to the daily operations of the Lotus Foundations server, which is especially important if you are using several features of the server at the same time. When a virus is encountered, it is cleaned up if possible. Otherwise it is renamed to filename-INFECTED and the user in whose directory the file was found is informed through email of the virus.

Mail virus scanner

AntiVirus for Lotus Foundations mail virus scanner scans all incoming and outgoing email messages, including attachments, for viruses. When mail messages that contain infected, suspicious, and other objects are detected, the virus is immediately removed and a warning is sent to the sender and recipient along with the original, but virus-free, mail message.

Activating your file virus scanner license

To activate your file virus scanner license, follow these steps:

1. Click **File Server** in the left side menu of WebConfig. The **Basic Setup** tab of the File Server Setup page is displayed.

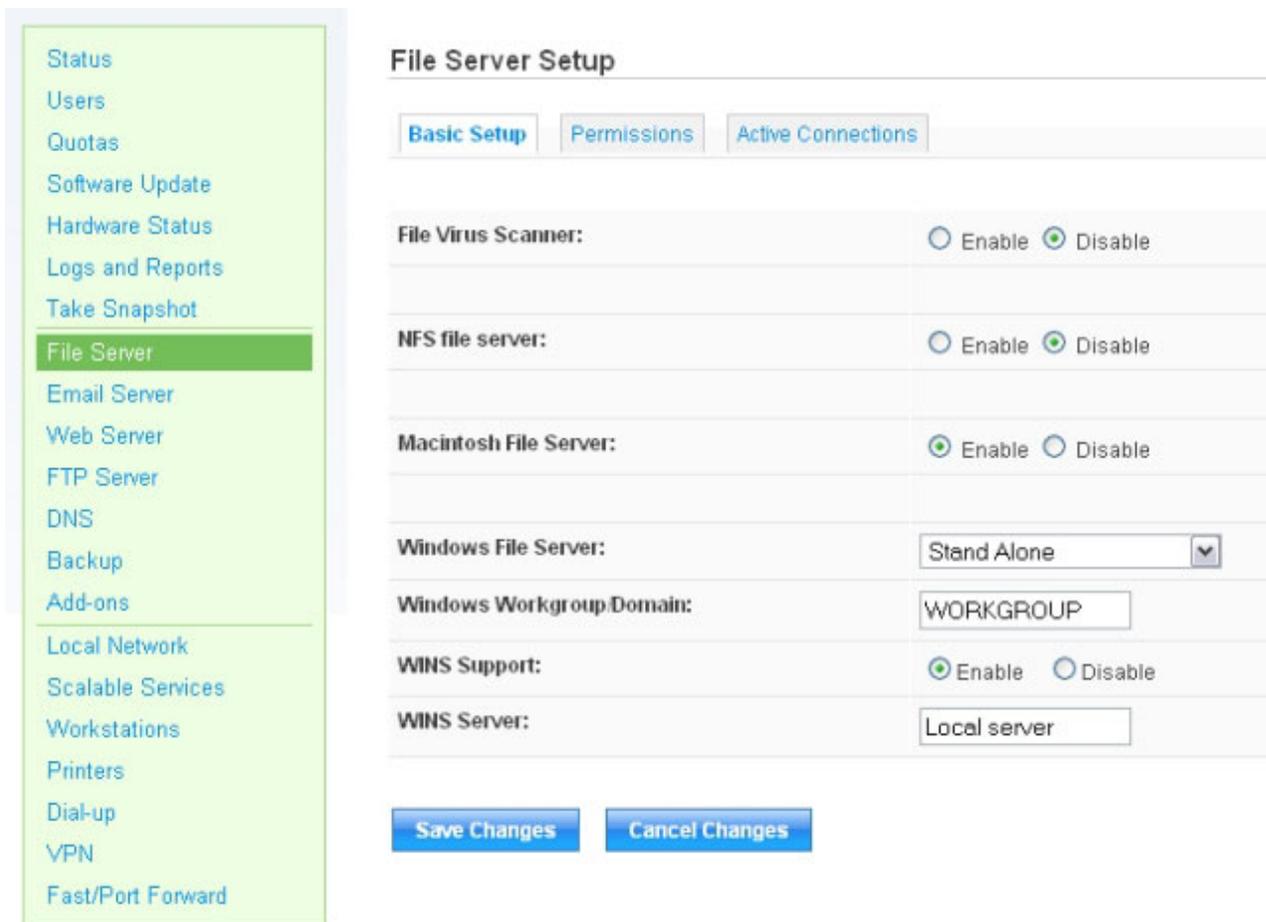


Figure 53. Basic Setup tab of the File Server Setup page of WebConfig

2. In the **File Virus Scanner** field, select **Enable**.
3. Click **Save Changes**.

Activating your mail virus scanner license

To activate your mail virus scanner license, follow these steps:

1. Click **Email Server** in the left side menu of WebConfig. The **Summary** tab of the Email Server Setup page is displayed.

Email Server Setup

Summary Servers Filters Monitoring Addressing Advanced Filtering

| Option | Status | Comment |
|-------------------------------------|--------|--|
| POP3 Server | ✓ | Trusted network only |
| POP3/SSL support | ✓ | Trusted network only |
| IMAP Server | ✓ | Trusted network only |
| IMAP/SSL support | ✓ | Trusted network only |
| SMTP Server | ✓ | Trusted network only |
| Virus Scan | ✓ | Virus scanning all emails. |
| Content Spam Scan | ✓ | |
| Network Spam Scan | ⚠ | No network filtering license is available. |
| RBL | ✓ | Medium |
| SMTP Authentication | ⌘ | |
| Smarthosting | ⌘ | |
| Attachment Filter | ⌘ | |
| Allowed Relays | ⌘ | |

Save Changes Cancel Changes

Figure 54. Summary tab of the Email Server Setup page of WebConfig

2. Click the **Filters** tab.

Email Server Setup

Summary Servers Filters Monitoring Addressing Advanced Filtering

Mail Virus Scanner: All Emails Inbound Only Disable ⓘ

RBL (spam blocker): Strong RBL Medium RBL No RBL ⓘ

Mail Spam Scanner: Enable Disable ⓘ

User White/Black Lists: Enable Disable ⓘ

Definite Spam Categories: Hoax Adult Money Goods Health ⓘ

Attachment Filter: Enable Disable ⓘ

Save Changes Cancel Changes

Figure 55. Filters tab of the Email Server Setup page of WebConfig

3. For the **Mail Virus Scanner** field, select **All Emails** or **Inbound Only** to activate mail virus scanning.

4. Click Save Changes.

Lotus Foundations Start performance optimization

With such a vast array of features, it can be challenging to determine how Lotus Foundations can be optimized for performance in specific deployment scenarios. How fast the processor should be, how much memory is required, and how often backups should run are all valid questions. With its robust application server, Lotus Foundations Start introduces even more questions when considering optimization.

This chapter explores some Lotus Foundations Start performance considerations to assist you in deploying Lotus Foundations Start as a robust, reliable, and efficient back-end server.

Minimum hardware requirements

The Domino server that sits at the heart of Lotus Foundations Start is a product built for enterprise scalability. While Domino initially requires a substantial pool of resources to be able to operate almost regardless of the number of users, the incremental resources required for each additional user is typically less than for traditional applications built for small deployments. Keep this in mind when choosing the hardware required to run the system.

Minimum requirements to run Lotus Foundations Start:

- 1 GB of memory
- Pentium® 4 3.0 GHz processor (or AMD equivalent)

To accommodate Domino, it is recommended that you use a system with SATA disks. For larger installations and/or installations with higher performance requirements, it is recommended that you use a system with higher-end SCSI disks.

The basic requirements are met with a Lotus Foundations Appliance or IBM System x3105. This server is capable of supporting 25 to 30 average users¹. Allowances should be made if your deployment environment differs significantly from the average, particularly with respect to the amount of email traffic and the size of the users' mail databases that are stored on the server.

Deploy Lotus Foundations Start on hardware as fast as your budget accommodates, particularly if you intend to deploy applications in addition to the standard email/groupware bundled with Lotus Foundations Start.

¹ The average email user sends and receives approximately 100-200 emails per day, and has a mail database of 500 MB. The average email is 50 KB in size. For calculation purposes, the average Lotus Foundations Start user uses a Lotus Notes client connected live to the server.

Quick reference and hardware sizing guide

The following table illustrates the recommended sizes based on number of users for optimum system selection:

Table 25. Recommended configurations based on number of users

| Number of users | Configuration used in baseline | Representative base hardware configurations | Notes |
|-----------------|--|---|------------------------------|
| 1 -5 | AMD Athlon64 3500+ 2.2 GHz, Intel® Pentium 4 3.2 GHz or greater, 100 GB SATA | Lotus Foundations Appliance | Requires external idb backup |

Table 25. Recommended configurations based on number of users (continued)

| | | | |
|---------|--|---|--|
| 6 -50 | Intel Core 2 Duo 2.0 GHz / 800 MHz Bus / 2 MB Cache (E4400), 1 GB DDR2 SDRAM (4 GB max), 2 x 250 GB removable SATA hard drives | IBM System x3105 or Lotus Foundations Appliance | 1 disk reserved for idb backup |
| 50 -150 | Intel Core 2 Duo 2.6 GHz / 1066 MHz Bus / 4 MB Cache (E6600), 2 GB DDR2 PC5300, 3 x 250 GB removable SATA hard drives | IBM System x3105 or Lotus Foundations Appliance | 1 disk reserved for idb backup |
| 150+ | Dual Intel Xeon® 1.86 GHz, 4 MB Cache, 4 x 1024 MB DDR2, 4 x 512 DDR2, 4 x 73.4 GB 10K SAS Drives (IBM P/N: 39R7340) | IBM System x3400 | For larger numbers of users, additional disk space is required for data storage, double backup and idb backup. Domino with 150 mail databases of 250 MB is 65 GB. Domino and 500 mail databases is 127 GB. Double backups requires the disk space requirement to be doubled. |

Email protocol choices affecting server performance

This section provides the major protocol choices provided to permit email clients to connect to the Lotus Foundations Start server and their relative impact on the server. This section includes the load required, based on relative system usage, to support the protocol, as well as any document conversions required to transmit the emails.

- Notes (local replication of mail database) - 0.5
- Notes (server copy of mail database) or Domino Access for Microsoft Office (DAMO) - 1
- Lotus iNotes - 3
- Internet Message Access Protocol version 4 (IMAP4) - 3
- IMAP4 over Secure Sockets Layer (SSL) - 3.5
- Post Office Protocol version 3 (POP3) - 2
- POP3 over SSL - 2.5

When determining the type of client to deploy, how many users, and type of users, the above demonstrates that not all clients are equivalent.

Other services running on the Foundations Server

Even if the server is used almost exclusively for email and email-related services, consideration must be given to services such as Spam Scanner and AntiVirus for Lotus Foundations. The load that these services place on the server is determined by the amount of external email received on the system. Resource planning should be based on the actual amount of email the system receives. In other words, include real email, viruses, and spam email a user receives during resource planning; do not just include the amount of legitimate email a user receives.

Careful consideration should also be given to the many other services running on the Lotus Foundations Start server, including the file server, Web server, and Point-to-Point Tunneling Protocol (PPTP).

Lotus Foundations Start requires approximately 1 GB of memory for Domino. If your system uses other services, consider upgrading memory to ensure that adequate memory is available to run services in addition to Domino.

The same consideration should be given to the processor selection: allowances should be planned so that other services may adequately run in conjunction with the Domino server.

Backup scheduling

Lotus Foundations Start includes an idb job that takes care of backing up the *notesbackup* team. This job is the LF Start Backup job. The job itself takes care of backing up the Domino databases safely to the *notesbackup* team each time the job runs so that the databases are in a consistent state when backed up. You should schedule the job for minimum impact on the business operations.

Carefully consider when a backup is scheduled to start and how often the backup is scheduled to run. You should gauge approximately how long your backups take based upon how much data you have.

The following should help you in your planning:

Table 26. Domino backup duration based on number of users

| Number of Users | Domino backup duration |
|-----------------|--|
| 20 | First backup approximately 60 minutes; subsequent backups approximately 15 minutes |
| 50 | First backup approximately 3 hours; subsequent backups approximately 1 hour |
| 150 | First backup approximately 3.5 hours; subsequent backups approximately 1.5 hours |

For example: If you have 20 users with a total email size of 5 GB and total disk space used on the system is 150 GB, you can expect the backing up the Domino databases part of the LF Start Backup job to take approximately 15 minutes. A full backup of the same system takes approximately two to three hours, plus another two to three hours to perform the backup verification (for a total of four to six hours).

Most offices like to perform their backups during off-hours, as backups place an extra load on the server. An example schedule assumes that you want the backups to start at some time after 9:00 PM and complete by 7:00 AM. If you schedule the LF Start Backup job to begin at 9:00 PM, with 5 GB of data, the estimated time to completion for the Domino database backups part of the LF Start Backup job would be 9:15 PM. Given the estimate that a full idb backup takes up to six hours to complete, the idb backup part of the LF Start Backup job should start no later than 1:00 AM. To provide a bit of margin (and a bit of room for growth in the database and system server usage), schedule the LF Start Backup job for 10:00 PM.

It might not always be possible to schedule the backups without impacting business operations, as the business might be open for extended time periods or the amount of data might require the backup windows overlap into the business day. In these circumstances, it is valuable to consider what time of the day the extra load would have the least impact on the business.

Future capacity planning

The storage space required on a server for files and email can rapidly increase. Anticipate your future needs and choose the correct hard drive capacities, but also be aware that increased capacities have an impact on your server performance. Effects of increased storage on server performance include the following:

- idb backups take longer to perform
- More memory and processor power required to process mail
- More memory and processor power required to process full text indexes (if enabled)

Ever-increasing size in users' mail databases can have a negative overall impact to the server. It is worth considering setting user email quotas to limit the growth of mail databases. Desktop clients, such as Notes, can be set to automatically archive older mail offline so that an archive of mail is still available without suffering the performance penalties associated with keeping the seldom-accessed old mail active on the server.

Domino is an application platform. If you intend to use applications, then considerations need to be made regarding disk capacity, processor, and memory to accommodate the needs of the applications. Each application has different system needs, so application documentation should be referenced for capacity planning.

Glossary

| | |
|------------------------------|--|
| ADSL | Asymmetric Digital Subscriber Line. ADSL uses standard phone lines to deliver high-speed data communications. ADSL uses the portion of a phone line's bandwidth not utilized by voice, allowing for simultaneous voice and data transmission. |
| Bandwidth | This term describes information-carrying capacity of telephone or network wiring. Bandwidth is usually measured in bits per second. |
| Bit | Binary Digit. The smallest unit of computerized data. A bit is represented as either 1 or 0. |
| Cable Modem | Cable modems provide Internet access over cable TV networks (which use fiber-optic or coaxial cables). They are generally much faster than modems that use phone lines. |
| Cache | A copy of a program or data that is used for faster access. See also Web Cache. |
| Certificate Authority | An issuer of security certificates used in SSL connections. See also SSL. |
| Client | A computer system or process that requests a service from another computer system or process. |
| Data Encryption | Encrypting data is accomplished by applying a scrambling code that makes the data unreadable to anyone who does not have a decryption key. Authorized personnel with access to this key can unscramble it. Data encryption is a useful tool against malicious users. |
| DHCP | Dynamic Host Configuration Protocol. This is an industry-standard protocol that assigns IP information to computers. |
| Disk Quota | Disk Quota defines the maximum amount of hard disk space allowed for a user's files. |
| DNS | Domain Name Service. A set of guidelines and rules that allows you to navigate the Internet using domain names instead of IP addresses. |
| DDNS or DynamicDNS | Dynamic Domain Name Service. A service that automatically updates DNS information when a new IP address is assigned to a network. |
| DNS Server | A computer or server that matches an IP addresses to a domain name. Some ISPs provide a specific DNS address. |

| | |
|-----------------------------|---|
| DSL | Digital Subscriber Line. Technology that provides data transmission over the telephone network. |
| Ethernet | A LAN that connects devices like computers, printers, and terminals. Ethernet transmits data over twisted-pair or coaxial cables at 10, 100, or 1000 Mbps. |
| EtherTalk | Networking protocol used by Apple equipment connected directly to Ethernet. |
| FastForward | The ability to create a passage (or open a port) through your firewall to a service or a server hosting a service. See also Port Number. |
| Firewall | A device that provides secure Internet access and protects internal networks from intruders. |
| FTP | File Transfer Protocol. An Internet based protocol used to copy files between computers (usually a client and a server) using UNIX-based command parameters. You can download shareware or freeware applications that remove all the complexities of UNIX and allow you to connect to FTP sites using a Web browser. |
| Gateway | A computer or server that is connected to multiple networks and is capable of routing or delivering packets between them. |
| HTML | Hypertext Markup Language. A set of tags and instructions used to create web pages. HTML tags create page layouts, format text, insert graphics and multimedia, and more. |
| HTTP | Hypertext Transfer Protocol. A protocol that makes hypertext information such as web pages available over the Internet. |
| Hub | A piece of hardware that connects computers together in a LAN, allowing information to travel between them. |
| Internet Gateway | A gateway for accessing the Internet, which is loosely defined as points of entrance to and exit from a communications network. A gateway is the node that translates between two otherwise incompatible networks or network segments. Gateways perform code and protocol conversion to facilitate traffic between data highways of differing architecture. A gateway can be thought of as a function within a system that enables communications with the outside world. |
| IMAP | Internet Message Access Protocol. A popular protocol that allows a client to access email without downloading it to a local computer. Used mainly to read email from a remote location. |
| IMAP Server | A server that uses IMAP to provide access to multiple server-side folders. |
| IP Address | Internet Protocol Address. The numeric address used to identify and locate a server, computer, or Web site on the Internet. |
| IP Address (Dynamic) | A temporary IP address that is assigned to a computer by a DHCP server each time it goes online. |

| | |
|----------------------------|---|
| IP Address (Static) | A permanent IP address that is assigned to a computer in a TCP/IP network. Network devices that serve multiple users, such as servers, routers, and printers, are usually assigned static IP addresses. |
| IPsec | Internet Protocol Secure. A type of secure connection between computers at different locations, creating Virtual Private Networks. See also VPN (Virtual Private Network). |
| ISDN | Integrated Services Digital Networking. A digital-communication networking system used for high-speed communication with the Internet. ISDN is available through most telephone companies. |
| ISP | Internet Service Provider. An organization that maintains a server directly connected to the Internet. Users who are not directly connected to the Internet typically connect through an ISP. |
| Java™ | Designed by Sun Microsystems, Java is a programming language for adding animation and other action to Web sites. To view web sites created with Java, your browser has to have Java enabled. |
| JavaScript™ | Designed by Sun Microsystems and Netscape as an easy-to-use supplement to Java, JavaScript code can be added to standard HTML pages to create interactive documents. Most modern browsers support JavaScript. |
| kbps | Kilobits per Second (thousands of bits per second). This is a measure of bandwidth, the amount of data that can flow in a given time, on a data transmission medium. |
| LDAP | Lightweight Directory Access Protocol. The LDAP server provides a directory of users' names and email addresses. |
| LAN | Local Area Network. A LAN links together computers that are in the same building. 10BaseT Ethernet is the most common LAN. See also Hub. |
| Mbps | Megabits per Second (millions of bits per second). This is a measure of bandwidth (the amount of data that can flow in a given time) on a data transmission medium. |
| MX Record | Mail Exchange Record. A DNS resource record type that indicates which host can handle mail for a particular domain. |
| NetBIOS | Network Basic Input Output System. A protocol for networking on IBM PC and compatible systems. |
| NAT | Network Address Translation. NAT enables one publicly visible IP address to refer to many IP addresses internally on a LAN, making it look like all traffic was generated by a single external IP address. |
| NFS | Network File System. A protocol developed by Sun Microsystems which enables a computer to access files over a network as if they were on its local drive. |
| NIC | Network Interface Card. An adapter card that physically connects a computer to a network cable. |

| | |
|-----------------------------|--|
| NTP | Network Time Protocol. An Internet standard protocol (built on top of TCP/IP) that assures accurate synchronization to the millisecond of computer clock times in a network of computers. Running as a continuous background client program on a computer, the NTP client sends periodic time requests to external time servers, obtaining server time stamps and using them to adjust the client's clock. |
| Packet | A unit of data transmitted over a network. Large chunks of information are broken up into packets before they are sent across the Internet. |
| Packet Filter | A filter that blocks traffic based on a specific IP address or type of application (email, FTP, Web), which is specified by port number. |
| Peer-to-Peer Network | A network where there is no dedicated server. Computers with access privileges can share files and peripherals with all other computers on the network. |
| PING | Packet InterNet Groper. A program used to determine if a server is functional. It sends small packets to the server, which replies with similar packets. |
| POP3 | Post Office Protocol version 3. A popular protocol used most often by ISPs for receiving email messages. POP3 servers enable access to a single Inbox (as opposed to IMAP servers, which provide access to multiple server-side folders). |
| Port Number | A number assigned to an application program running on a computer in a TCP/IP-based network such as the Internet. The number is used to link the incoming data to the correct service. There are several standard port numbers. For example, port 80 is used for Web traffic. |
| PPP | Point-to-Point Protocol. A method of transmitting protocols (such as IP) over a serial link. PPP is most often used in dial-up modem connections from a home computer to an ISP. |
| PPPoE | Point-to-Point Protocol over Ethernet. PPPoE is often used to connect DSL providers. Because it is based on two common standards (PPP and Ethernet), it is easy to integrate into existing networks. |
| PPTP | Point-to-Point Tunneling Protocol. PPTP ensures secure communications over Virtual Private Networks. |
| Protocol | A set of rules that govern network exchanges. |
| Proxy Server | A server that acts as a barrier between an internal network and the Internet. Proxy servers can work with firewalls, which help keep outside users from gaining access to confidential information. A proxy server also enables the caching of Web pages for quicker retrieval. |
| RBL | Realtime Blackhole List. A 'spam' blocker that has different levels of spam protection (such as Strong or Medium). |
| Router | A device that handles the connection between two or more networks. |
| Routing | The act of directing packets between networks. |

| | |
|-----------------------------|--|
| Routing Table | A list of destinations known to the router (server) that enables user traffic to get to and from its destinations. |
| RSA | Rivest Shamir Adleman. An Internet encryption and authentication system that uses an algorithm developed by Ron Rivest, Adi Shamir, and Leonard Adleman. |
| Security Certificate | Information used by the SSL protocol to establish a secure connection. Contains information about who a certificate belongs to, who issued it, its unique serial number, its valid dates, and its encrypted 'fingerprint' that is used to verify the contents of the certificate. See also SSL. |
| Server | A computer or software package that provides specific services to a client. The term can refer to a particular piece of software (such as a Web server) or to the machine on which the software is running. A single server can run several different server software packages. |
| SNMP | Simple Network Management Protocol. A protocol used to collect statistical information from a host about parameters such as central processing unit (CPU) utilization. |
| SMTP | Simple Mail Transfer Protocol. A protocol used for transferring or sending email messages between servers. Another protocol (such as POP3) is used to retrieve the messages. |
| SQL | Structured Query Language. A language used to create advanced databases. |
| SSL | Secure Sockets Layer. A protocol that enables encrypted, authenticated communications to travel across the Internet. SSL is used mostly in communications between Web browsers and Web servers. URLs that begin with https indicate that an SSL connection is being used. Each side of an SSL connection must send a valid Security Certificate to the other. Each side then encrypts what it sends using both certificates, thereby ensuring that only the intended recipient can de-crypt it, that the other side can be sure of the data's origin, and that the message has not been tampered with. |
| Subnet | A portion of a network (which can be a physically independent network segment) that shares a network address with other portions of a network. A subnet is distinguished by its own subnet number. |
| TCP/IP | Transmission Control Protocol/Internet Protocol. A popular suite of protocols that allow computers to communicate on the Internet. |
| Telnet | An application that lets you access resources on a UNIX or Linux computer. To use Telnet, you need to be familiar with UNIX-based programs. |
| UDP | User Datagram Protocol. A protocol used throughout the Internet for services such as DNS. |
| URL | Uniform Resource Locator. The standard method to give an address of any resource on the Internet. A URL looks like this: (http://www.ibm.com). |

| | |
|-----------------------|--|
| VPN | Virtual Private Network. VPNs enable communication between users in different offices. To prevent people on the Internet from intercepting transmissions, all information that passes through a VPN is protected with 128-bit encryption, the strongest encryption technology available. |
| WAN | Wide Area Network A network that connects different LANs using routers. |
| Web Browser | An interface that lets you view material on the Internet. The most popular web browsers are from Microsoft and Netscape. |
| Web Cache | An area on your hard disk that is reserved for storing images, text, and other files that have been viewed on the Internet. |
| WebConfig | Web-based configuration system for Lotus Foundations. To connect to WebConfig, enter (http://hostname:8043) in the address bar of a Web browser. For example, if your Lotus Foundations server's host name is thunder, enter (http://thunder:8043) in the address bar. |
| WebMail Server | A system that enables users to access their email account using any standard Web browser. |

Note

As part of your purchase of IBM Lotus Foundations, you are also entitled to a full copy of SUSE Linux Enterprise Server (SLES) 10.1 operating system from Novell. You only need this if you need to modify your server with additional applications that require components from SLES that are not already integrated with Lotus Foundations. However, these extensions and applications are not a supported feature of IBM Lotus Foundations. To request a copy of SLES 10.1 send an email with your request to IBMLotusFoundations_Ops@us.ibm.com. Please include the following: contact name, company name, street address, city and postal code, country, contact phone, and contact email address.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not grant you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation
Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106-0032, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Office 4360
One Rogers Street
Cambridge, MA 02142
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement or any equivalent agreement between us.

Trademarks

IBM, the IBM logo, ibm.com, Lotus, and Notes are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. These and other IBM trademarked terms are marked on their first occurrence in this information with the appropriate symbol (® or ™), indicating US registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at <http://www.ibm.com/legal/copytrade.shtml>

Java and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux is a registered trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft and Windows are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX is a registered trademark of The Open Group in the United States and other countries.

Other company, product, or service names may be trademarks or service marks of others.