

Setting up a managed Secure File Interchange

Create secure networks over the Internet with just USB flash memory keys and an Internet connection.

Verisign estimates that it takes approximately 3 months and an enormous amount of money to set up a secure public key system. Please see their words at:

<http://www.verisign.com/static/005321.pdf>

<http://www.wnlabs.com/Presentations/TCO.pps>

Setting up a managed Secure File Interchange network from Whitenoise takes about half an hour.

1. You purchase keys for each of your employees.
2. You receive a unique Internet portal address for your secure network like <http://sfi.wnlabs.com> from a service provider.
3. The system administrator issues keys to each employee. It is like handing out an employee badge.
4. The application is set up for each employee by clicking the Setup.exe from their key from their USB flash memory drive.
5. The company system administrator (this does not have to be an “IT” person) trains the employees in half an hour how to logon to their key, how to logon to their Secure File Interchange portal, and how to send and receive authenticated and secure files.

Setting up a self contained Secure File Interchange for your enterprise

Create secure networks over the Internet with just USB flash memory keys, a simple server application and an Internet connection.

1. You purchase keys for each of your employees and you purchase the Secure File Interchange software for your own server.
2. You create a unique Internet portal for your secure network like <http://sfi.wnlabs.com>.
3. You install the server software onto your server by clicking Setup.exe on the server console software.
4. The system administrator issues keys to each employee. It is like handing out an employee badge. The system administrator assigns different permissions to each employee.
5. The application is set up for each employee by clicking the Setup.exe for their key from their USB flash memory drive.

- The company system administrator (this does not have to be an “IT” person) trains the employees in half an hour how to logon to their key, how to logon to their Secure File Interchange portal, and how to send and receive authenticated and secure files.

The entire process of issuing keys, adding and removing users, and assigning different permissions to each employee is as easy as filling out the following form:

The screenshot shows a web application interface with a navigation menu at the top containing 'Users', 'Classes', 'Groups', 'Keys', 'Logs', 'Tools', 'E-Mail', and 'Links'. The 'Users' tab is selected. Below the navigation menu is a 'User Details' section for a user named 'Admin'. The user information is as follows:

Username:	Admin
First Name:	Ants
Last Name:	Luts
e-Mail:	ants.luts@gmail.com
Description:	System Administrator Test
State:	Active
User Key:	06E03B4101E37FA5.key

Below the user information is a 'Classification' section with the following details:

Class:	Administrators
Theme:	Default
Maximum Storage:	52,428,800 bytes
Administrator:	Yes
Diva Required:	Yes
Items Per Inbox:	20
Items Per Groupbox:	10
e-Mail from Admins:	Yes
e-mail from Users:	Yes
e-mail from Groups:	Yes
Save Sent Copy:	Yes

At the bottom of the user details section are five buttons: 'Edit', 'Delete', 'Reset Password', 'Reset Diva', and 'Back'. The footer of the application displays 'Copyright 2006 - version 0.1 ALPHA'.