

**Tutis biometric logon is an elegant, robust, and scalable solution that uses biometric authentication for desktop and network access. Biometric authentication eliminates the need for remembering complex passwords and periodic changes to the password mandated by password management practices.**

### Biometric Authentication for Computers and Network Access

Authentication by computer systems to organization's network and resources usually takes the form of username and password dialog. The common problem with the password is that one tends to forget it. To avoid forgetting the passwords, it is either written down, or very simple password is used; in latter case, it can be guessed very easily thereby compromising security of the system. Periodic changing of password, enforced by administration, makes remembering even more difficult for complex passwords. Using biometric authentication instead of password avoids these problems and strengthens the security of the system.

### Biometric Logon

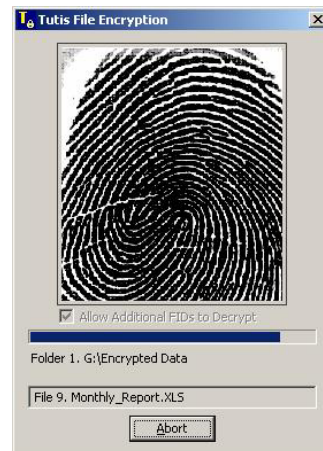
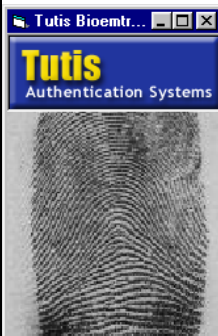
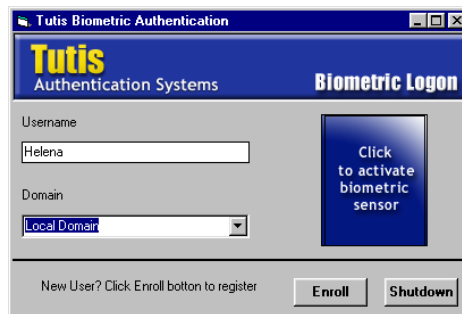
**Tutis** Biometric Logon provides authentication service using biometrics, which augments the traditional password based authentication. **Tutis** Biometric Logon system uses fingerprint of a person to authenticate and allow access to the local computer or network resource. It replaces the common username / password dialog with username / fingerprint dialog for logging to the desktop or the domain server.

**Tutis** Desktop Edition is used for authentication on a single machine whereas the **Tutis** Enterprise Edition is used for authentication over the network domain logon. The users need to enroll themselves using the simple enrollment option, once for every domain they logon on to. Once enrolled, the users will not be required to remember the password for logon. The two samples of a fingerprint captured during enrollment are stored as complex mathematical representations of the biometric (i.e., fingerprint) called templates. The original biometrics can not be reconstructed from stored template. In addition, the templates are encrypted to prevent any unauthorized access to these. User can enroll them using their specific desktops or request the administrator to enroll them through Admin Console.

For users who logon to the same domain using the same username frequently, the Rapid Access Mode provides a convenient way of logon. This Mode uses only the fingerprint for the purpose of authentication.

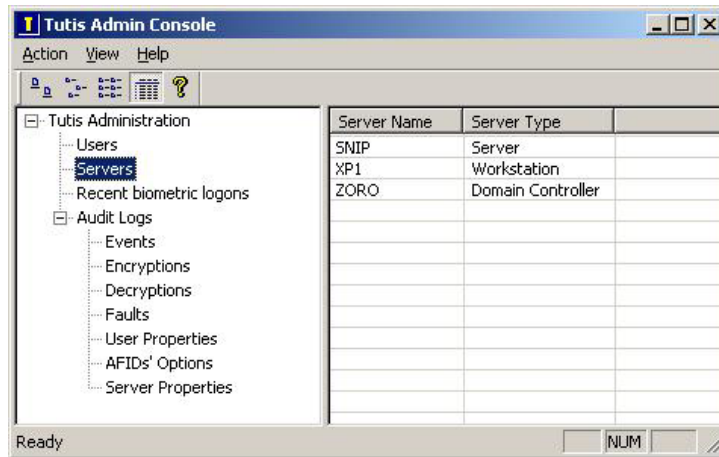
### Encryption

**Tutis** Encryption allows the users and AFIDs (additional fingerprint identifiers) to encrypt files. The encrypted files are called **Tutis** files, which are normal files and can be sent via email, through FTP, etc. The user (or AFIDs, if allowed) can only decrypt these files only after the fingerprint matches. Thus **Tutis** files are highly secure, portable and easy to use.



## Administration

User and server administration is extremely simple and intuitive. Administrator can set or



change properties for a specific server on the network including local machine. When the backup or secondary domain controllers are on the network, **Tutis** automatically replicates the database across domains. Similarly, properties for specific users can be set or changed. **Tutis** registers all the activities including faults in audit logs to help administrators.

## Features

- **Active Directory Support**
- Roaming users and profiles supported.
- Secured, encrypted storage of biometric records.
- Encrypted wire transfers for authentication between servers.
- Rapid Access Logon feature for frequently logged on accounts.
- Locking of Client PC using Admin Management Console.
- Protects unattended desktop with a fingerprint screen saver.
- Remote administration of workstations through Administration tool.
- Support for backup and/or secondary domain controller.
- Easy deployment and administration.
- Scalable, robust and secure.
- Option for display / hide the fingerprint image while capturing.
- Small footprint for Desktop as well as Enterprise versions.
- Support for multiple biometric devices.
- Support for multiple fingerprints for a Windows user account.
- File encryption with multiple fingerprint support.
- User-friendly browser for viewing Tutis activities.
- Tutis encrypted files can be transferred and decrypted on any Tutis system.

## Supported Operating Systems

- Microsoft Windows 2000 professional (SP 4).
- Microsoft Windows 2000 Advanced Server (SP 4).
- Microsoft Windows XP Professional and home edition (SP 2).
- Microsoft Windows 2003 Advanced Server (SP 1).

## Hardware Requirements

### **Tutis** Enterprise Edition Server

Pentium III or higher with minimum 128 MB RAM and 50 MB of free hard disk space.

### **Tutis** Desktop or clients

Pentium III or higher with minimum 32 MB RAM and 25 MB of free hard disk space. Appropriate supported biometric sensor is required on the clients as well as server.