# Everest Security Features

## Introduction

The Everest™ Web and Desktop Editions offer flexible, easy to use and powerful capabilities to medical and pharmaceutical companies focused on tracking product related complaints, ensuring complaint resolution, understanding quality issues and tracking corrective actions. This document describes security features required to ensure data security, authenticity and integrity.

## Login Security

EVEREST takes extensive precautions to ensure that only authorized users can access, edit and sign records.

- Every user requires a unique login Id and Password.
- Organizations can specify a minimum number of characters required for the password.
- Organizations can also specify the appropriate password aging days.
- Users will be automatically logged out of the system after a specified period of time.

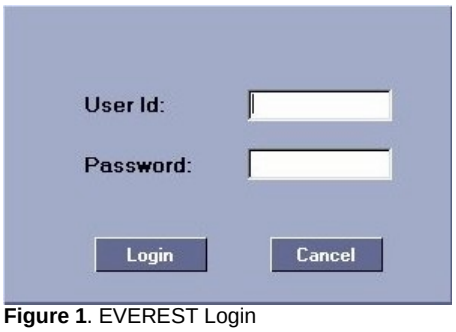


**Figure 1**. EVEREST Login

Note: Organizations that wish to follow FDA CFR Part 11 guidelines should not enable the auto logon feature of the Everest Desktop Edition.

## Electronic Signatures

Everest can be configured to require an approval and electronic signature to close a concern or corrective action record.

- Approvals: A check box will be enabled within the concern or corrective action. This box can be checked by any user that is in a User Group with 'Perform Approval' privileges.
- Approvals with Electronic Signature: This will require that the user enter their password when approving a concern or corrective action.
- Approvals with Electronic Signatures and Dual Passwords: This will require that a user maintain a separate and distinct password for approving a concern or corrective action.

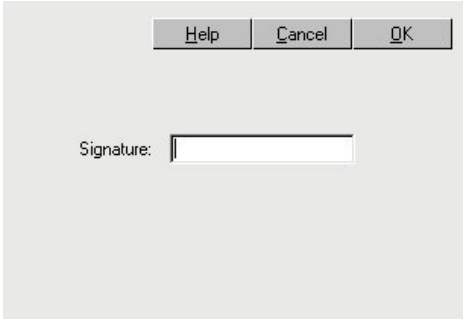


**Figure 2.** Electronic Signature

**User Group Controls**


In addition to extensive control of the logon process, user access and privileges are also controlled from within the application.

Each user is a member of a User Group that will determine his/her access privileges.

By default only a 'Concern Owner' or 'Action Owner' can edit their own records. Additional privileges such as the ability to have Full Access to all Concerns or to Perform Approvals will be tightly controlled.

End users do not have access to the setup menu to view or edit these privileges.

**Audit Report**

EVEREST maintains a time-stamped audit trail that contains every Add, Edit or Delete to a concern and corrective action record. This is an optional feature that can be turned on in Setup | Configure Options | Other Options.

**Date Retention and Security**

Within Everest data can be retained for any specified amount of time. The Everest data is stored in a standard non-proprietary database (either MS Access or MS SQL Server). This database should be physically and electronically secured and backed up on a regular basis.

**Software Validation**

Lynk Software offers a complete IQ/OQ procedure that can be used by our clients to document and validate the Everest software.

## Important Information

This document is not legal advice or legal standard. Companies must ensure that their individual practices and procedures comply with the requirements of third party regulatory agencies and may wish to obtain legal advice from a qualified attorney on this topic. Lynk Software, Inc. assumes no responsibility or liability for the regulatory compliance of Everest users.