

Get Protected in Four Easy Steps

First Step: Enterprise Security Installation

Enterprise Security will do the hard work for you.

- Automatic implementation
- Logging and full monitoring

Second Step: Implementation

Change the System Policy to reflect the permissions you plan to give to most groups. This will act as a template when creating new permissions and so make the jobs of setting up permissions easier and simpler.

- Under the **Application Access Control** heading mark the checkbox beside the applications and functions to be given the majority, clear the checkbox where the applications and functions are not needed by most users.
- Under the **Unauthorized Access** heading, Make sure **Warning** appears next to all the application servers. If **Reject** appears for any of these, change it to **Warning**. This will ensure the system runs in warning or simulation mode.

Status analysis and implementation (use the Application Analyzer to assist you in the task)

- Review all active users and group them by their application access requirements.
- For each group you have identified, create a user group using the Enterprise Security Group Manager and assign the users to the groups. If you have users who you are unsure of which group they belong, create a general group and assign them to it. You can make changes like removing users from one group and assigning them to another at any time.
- Create the permissions for each group in the Application Access function. Allow access only to the application servers and functions they will need.

IP Address Permissions

- Define IP address ranges using IP Address Network Manager by areas according to territory in the network (see IP addresses used by using the Select From Log button on the Add IP Range screen)
- Assign Telnet permissions to active permitted IP address ranges only.

Change the System Policy to lock out all access outside of the permissions you have defined

- Under the **Application Access Control** heading, clear the checkbox beside most and preferably all of the applications. Only applications and functions which you want to be available to users who do not have specific definitions should be marked.
- Under the Log Recording title, select **Violation** next to every application server.

Third Step: Application Audit log and Monitoring Control

- Check whether simulated log warning in the audit log is correct and as expected to be (using Application Audit Log and Application Analyzer).
- Adaptation/addition/deletion of permissions as required.

Fourth Step: Fix System Policy

- Verify that log results coincide with the permissions policy.
- If log results are correct and according to expectations – change status “on unauthorized access” vector in the system policy from simulation (**Warning**) to read rejection (**Reject**).

Note: For better control and minimum maintenance it is recommended to avoid using restrictions by users and preferable to use permissions by user group instead.

The method above described is simple, efficient and cost saving. All internal and external organizational activity in communications is prohibited and only permissions according to real activity are allowed.

A more expansive description of this task may be found in **Implementing Enterprise Security Protection** available in the Implementation.pdf

Now your system is fully protected and under Enterprise Security control.