

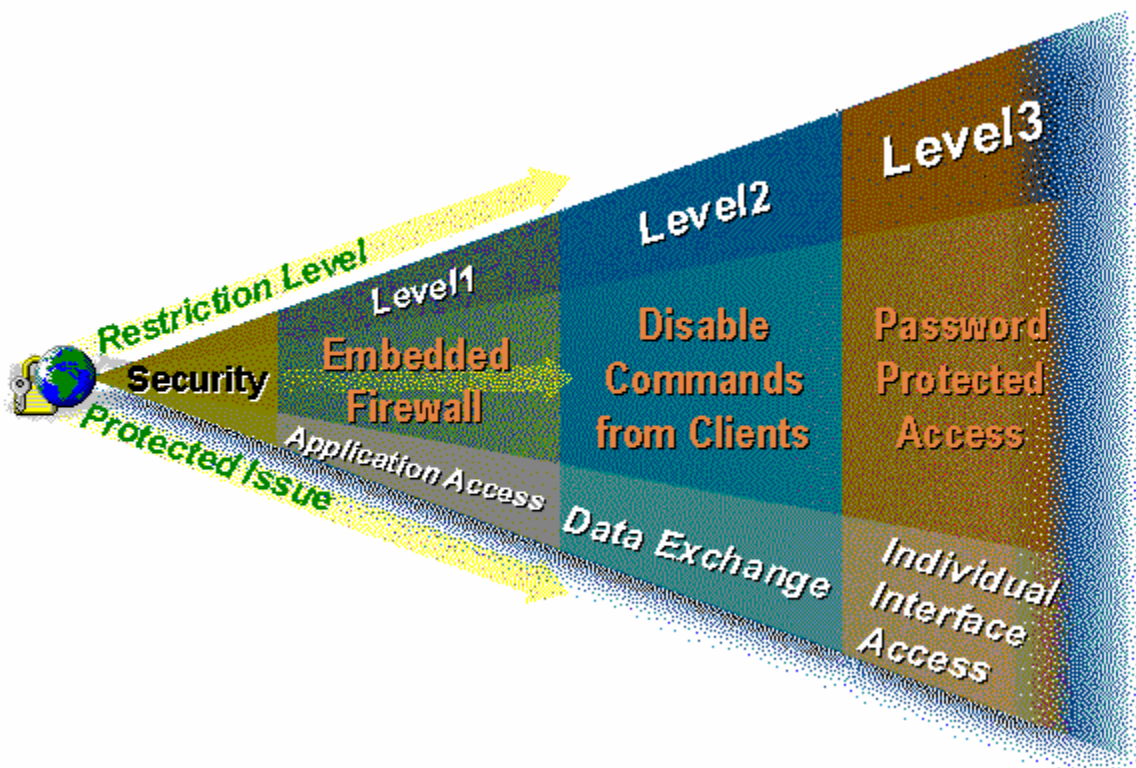
IWS Security System for Web-based Applications

I. Introduction

The security issue of Web Based Applications (WBA) is an important topic. The aim of this document is to explain how to configure the security system of Studio for WBA.

Studio provides three levels of protection for its WBA that allows you to configure a flexible, powerful and secure architecture that avoids unauthorized access to your application while remaining running in the Server station:

- Level1: Embedded Firewall → Application Access
- Level2: Disable Commands from Clients → Data Exchange
- Level3: Password Protected Access → Individual Interface Access



It is important to clearly indicate that each one of these levels can be individually enabled/disabled, according to the user configuration. Also, all of them can coexist in the same application at the same time.

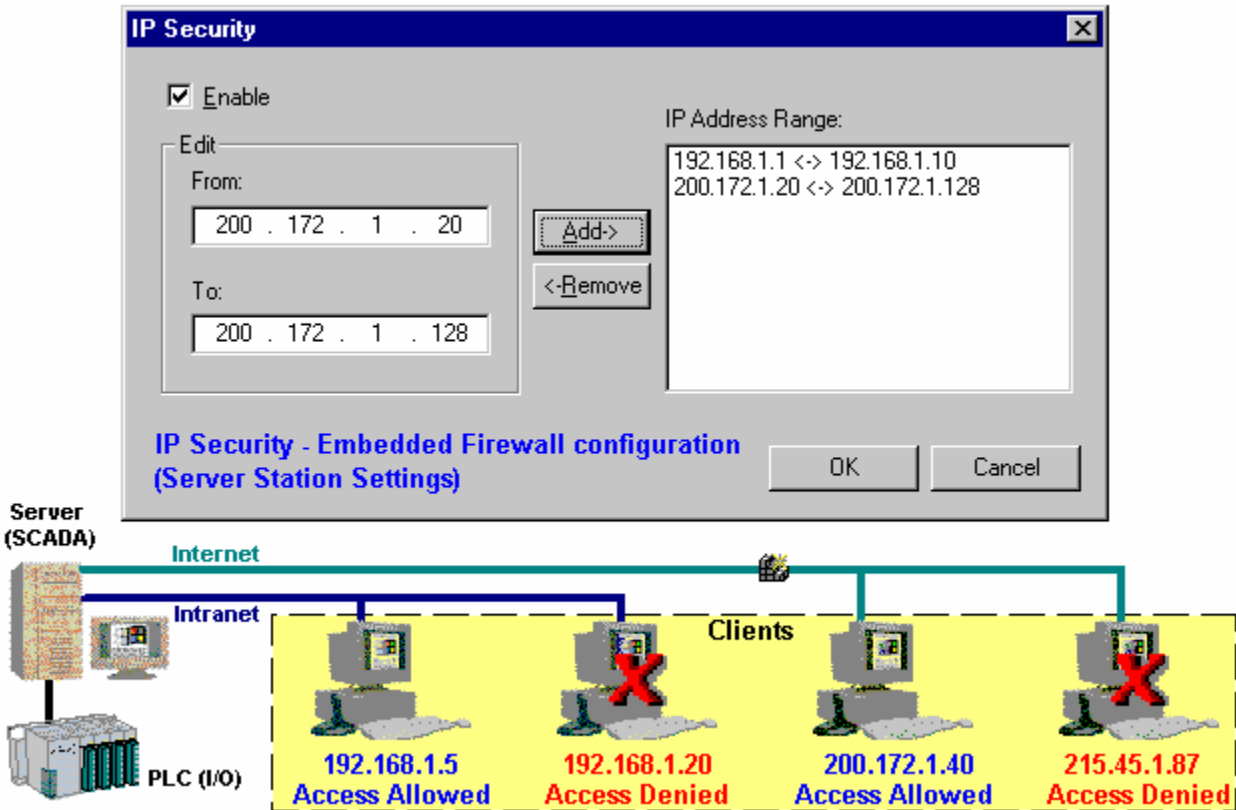
The access control is managed by the Server station and the security system settings cannot be modified remotely to guarantee major reliability to the whole security system.

Note: The picture above illustrates the tools available in Studio to protect the WBA. Additional standard protections (firewall for web access, anti-virus packages, etc) can run independently of the Studio security system and guarantee major security to the overall system.

II. Level1 – Embedded Firewall

This feature allows the user to filter access to the application based on the Web Thin Clients IP Address. When the Web Thin Client attempts to connect to the Server station, it checks if the IP Address of the Web Thin Client station is authorized to access the application.

The ranges of authorized IP Addresses can be configured in the Server station, pressing the **IP Security** button from the **Project** → **Settings** → **Web** dialog window of the Studio development environment:



The screenshot shows the **IP Security** dialog box with the following configuration:

- Enable**
- Edit** section:
 - From:** 200 . 172 . 1 . 20
 - To:** 200 . 172 . 1 . 128
- IP Address Range:** 192.168.1.1 <-> 192.168.1.10, 200.172.1.20 <-> 200.172.1.128
- Buttons: **Add->**, **<-Remove**, **OK**, **Cancel**
- Text: **IP Security - Embedded Firewall configuration (Server Station Settings)**

The network diagram below shows a **Server (SCADA)** connected to an **Intranet** and the **Internet**. The **Internet** is connected to a group of **Clients**. The **Intranet** contains a **PLC (I/O)**. The **Clients** are shown with their IP addresses and access status:

Client IP Address	Access Status
192.168.1.5	Access Allowed
192.168.1.20	Access Denied
200.172.1.40	Access Allowed
215.45.1.87	Access Denied

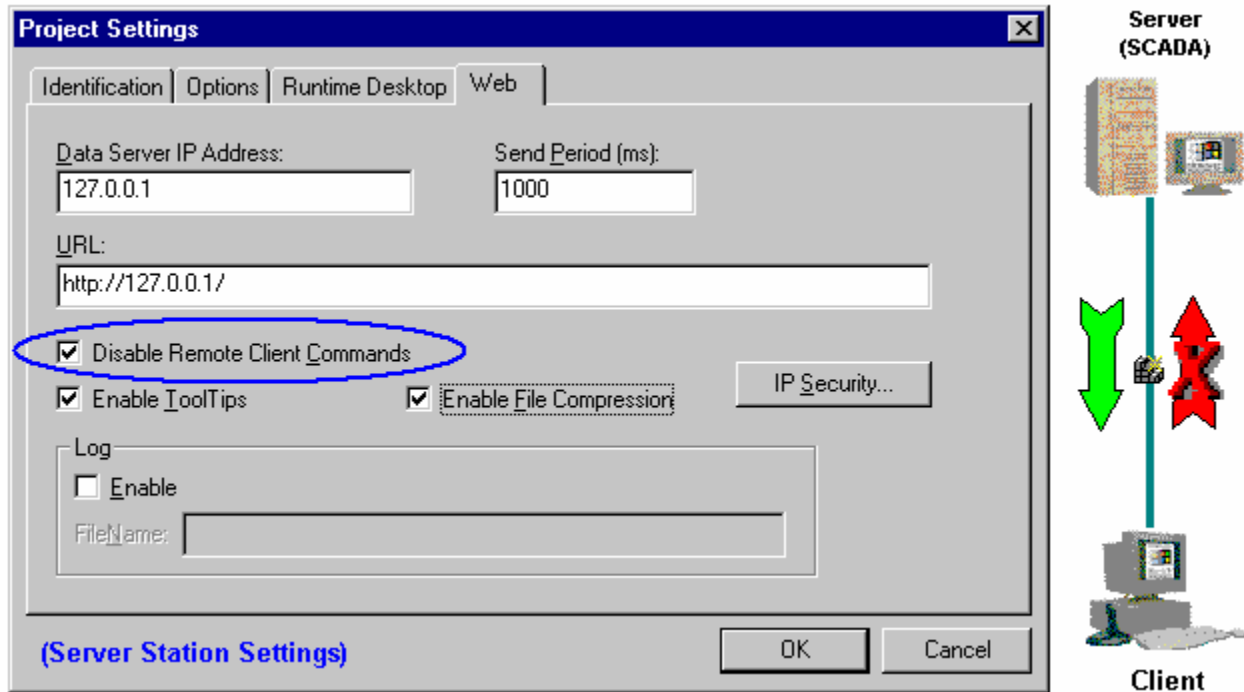
If the Web Thin Client IP Address was not previously configured in the *IP Address Range* list of the Server station, the Web Thin Client station will not have access to the Server application at all (visualization and data exchange).

Note: This feature is useful when the Web Thin Client stations are networked in an Intranet where the IP Address of each computer can be easily configured. When the Web Thin Client station is connected to the Server via the Internet, the IP Address assigned to the Web Thin Client station by the ISP is usually dynamic (not a fixed IP Address). In this case, it will not be possible to have control on the Web Thin Client IP Addresses and it may not be feasible to apply this security system level to the application.

III. Level2 – Disable Commands from Clients

Studio provides bi-directional data exchange between the Server and the Web Thin Client stations. However, in some applications, it is desired that the Web Thin Client stations only visualize information from the process (from the Server) and not any send data to the server.

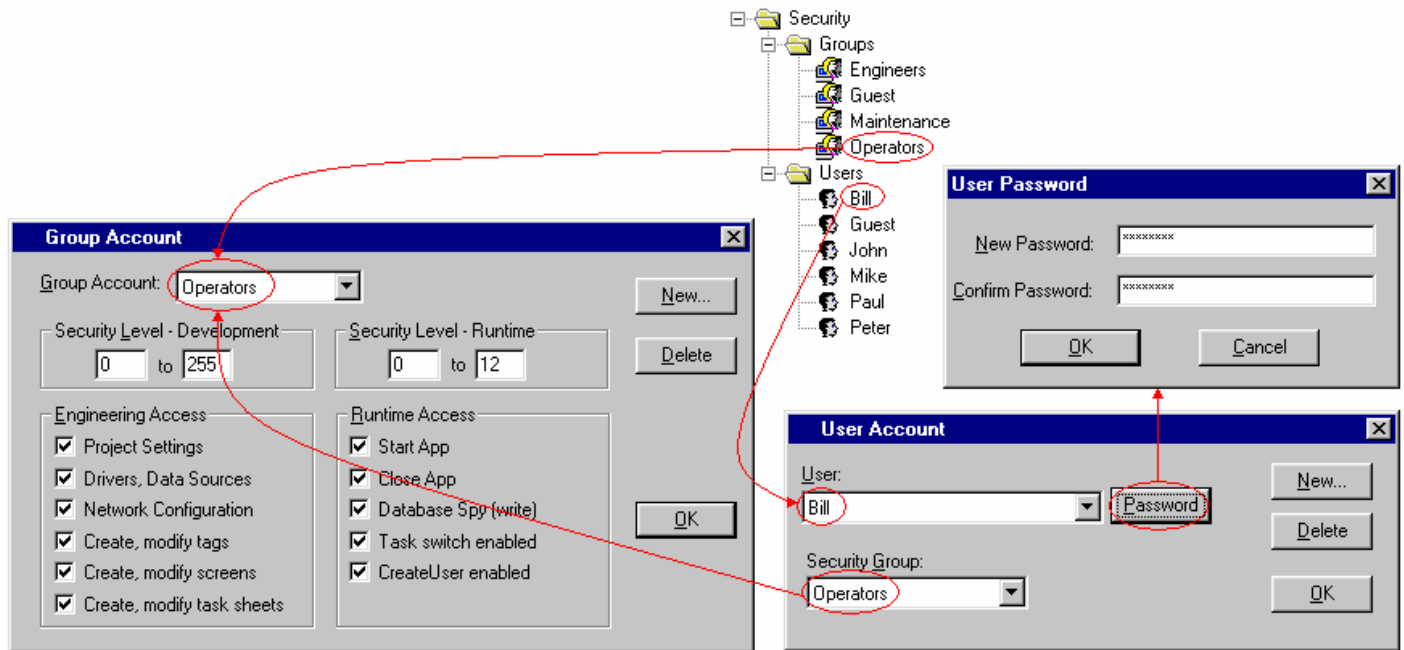
Checking the **Disable Remote Client Commands** check-box from the **Project Settings** → **Web** dialog window of the Studio development environment insures all commands from the Web Thin Client station are blocked. In other words, the communication becomes unidirectional (from the Server to the Web Thin Clients):



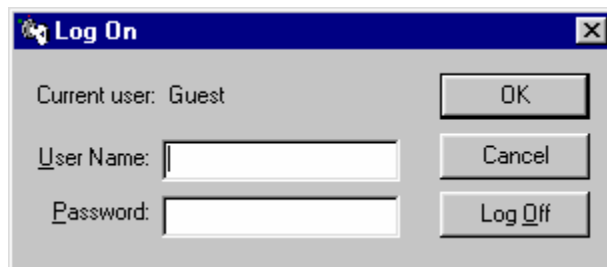
It is an easy-to-use tool to prevent the application from any command from the Web Thin Client station.

IV. Level3 – Password Protected Access

This is the most flexible level to protect the application. Studio provides an interface to create several Groups and configure the rights and restrictions of each group. Then, several users can be created for each group and the rights and restrictions configured for each group are applied for their users. A password can be configured for each user.



When the Web Thin Client station attempts to connect to the Server station, it automatically prompts a dialog window in the browser, requesting the User name and Password.

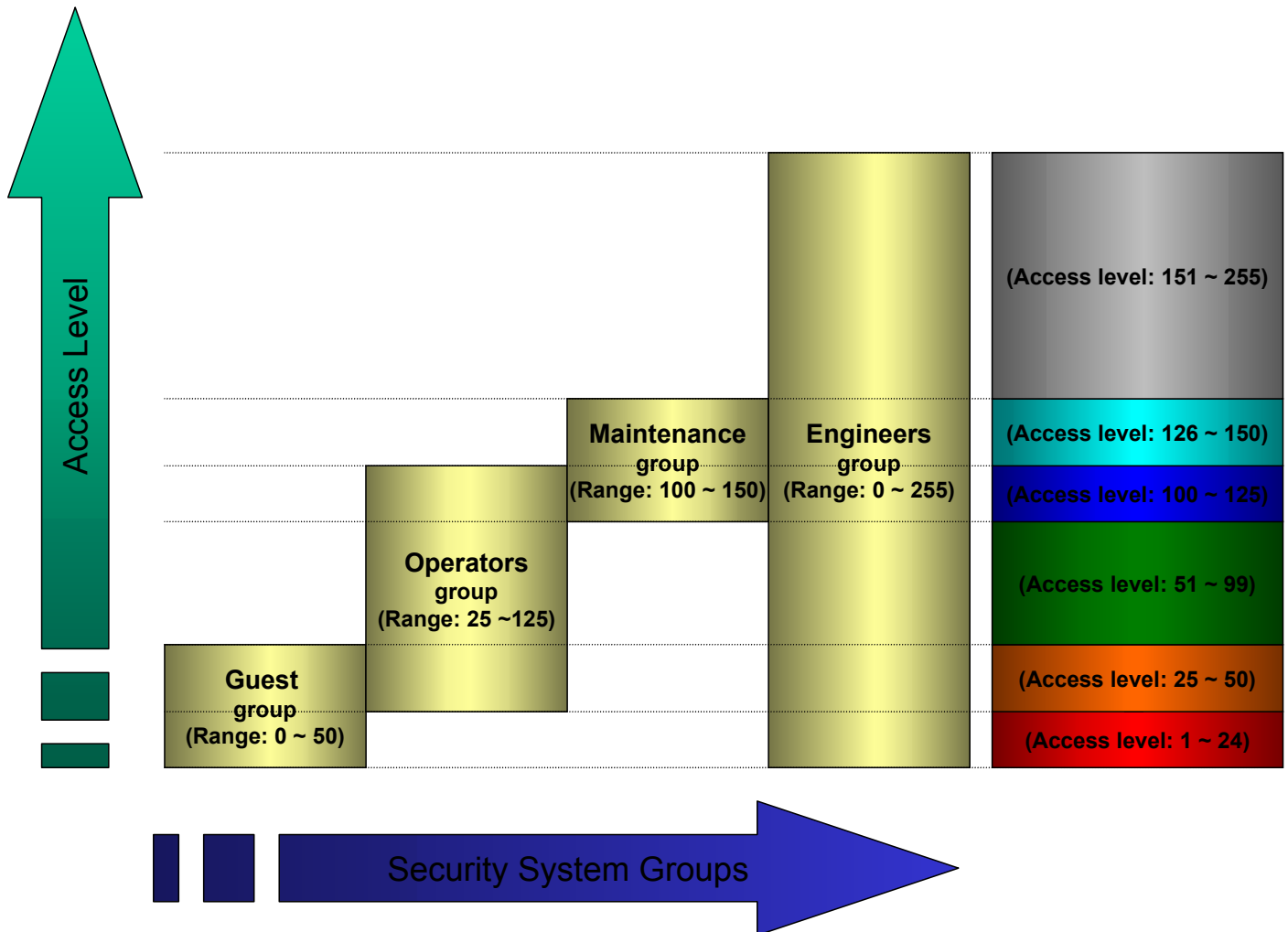


If the user will not enter a valid User name and Password, the Web Thin Client station will not have access to the Server application at all (visualization and data exchange).

Otherwise, the user will have the rights and restrictions configured in the Server for the user that was logged in the Web Thin Client. The Server station can handle different clients logged in different Web Thin Client stations simultaneously. Moreover, the security system is valid for both local and remote access to the application. Therefore, since the security system was configured for local access in the application, the settings are automatically applied to the Web Thin Client stations.


When the objects and dynamics are configured on the application screens, each object can be configured with a specific Access Level. Therefore, it is possible to enable access to each dynamic (Command, Text I/O Input and Slider) of each object on the screen for some users and disable them for others.

Since each Group can be configured with a range of Access Level, it provides a flexible and powerful tool to enable/disable access for each object on the application screens.



According to the example above, users from the **Guest** group can input new values to trigger commands for objects configured with the Access Level from 1 up to 50. Users from the **Operators** group can input new values to trigger commands for objects configured with the Access Level from 25 up to 120, and so on.

For instance, if a button with **Command** dynamic to open a valve is set with Access Level=110, this valve can be opened by users from the **Operators**, **Maintenance** and **Engineers** groups, but cannot be opened by users from the **Guest** group. If a set-point input field is set with Access Level=160, only users from the **Engineers** group are allowed to input a new value to this set-point.

 **Tips:** When an object is configured with Access Level=0 (default), all users are able to trigger actions to this object.

V. Map of Revisions

Revision	Author	Date	Comments
0	Fabio Terezinho	May 20, 2000	Initial revision
A	Fabio Terezinho	November 1, 2001	Overall layout revision
B	Fabio Terezinho	October 3, 2003	Layout revision