

Segurança no iFix

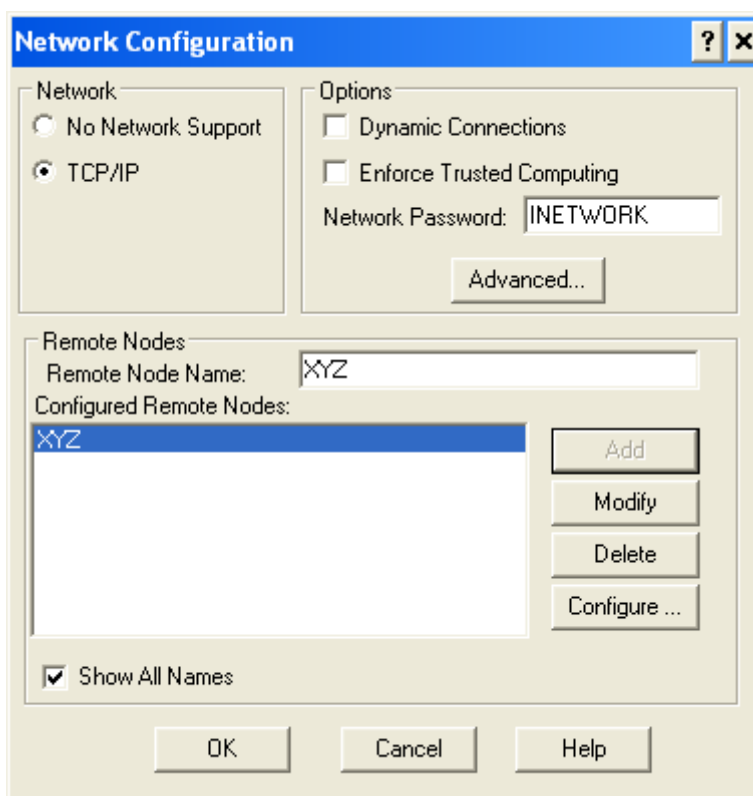
por Diogo Gomes

A configuração de segurança do iFix pode ser dividida em 3 partes principais:

1. Restrição de acesso entre estações Clientes/Servidor

Podemos configurar duas ou mais arquiteturas cliente/servidor, em uma mesma rede, através da definição de uma chave de acesso, tornando-as isoladas, como se estivessem em redes separadas.

Dentro do utilitário de configuração do sistema (SCU), na área de configuração de rede, configure o campo "Network Password", com um nome único em todas as máquinas de cada arquitetura.

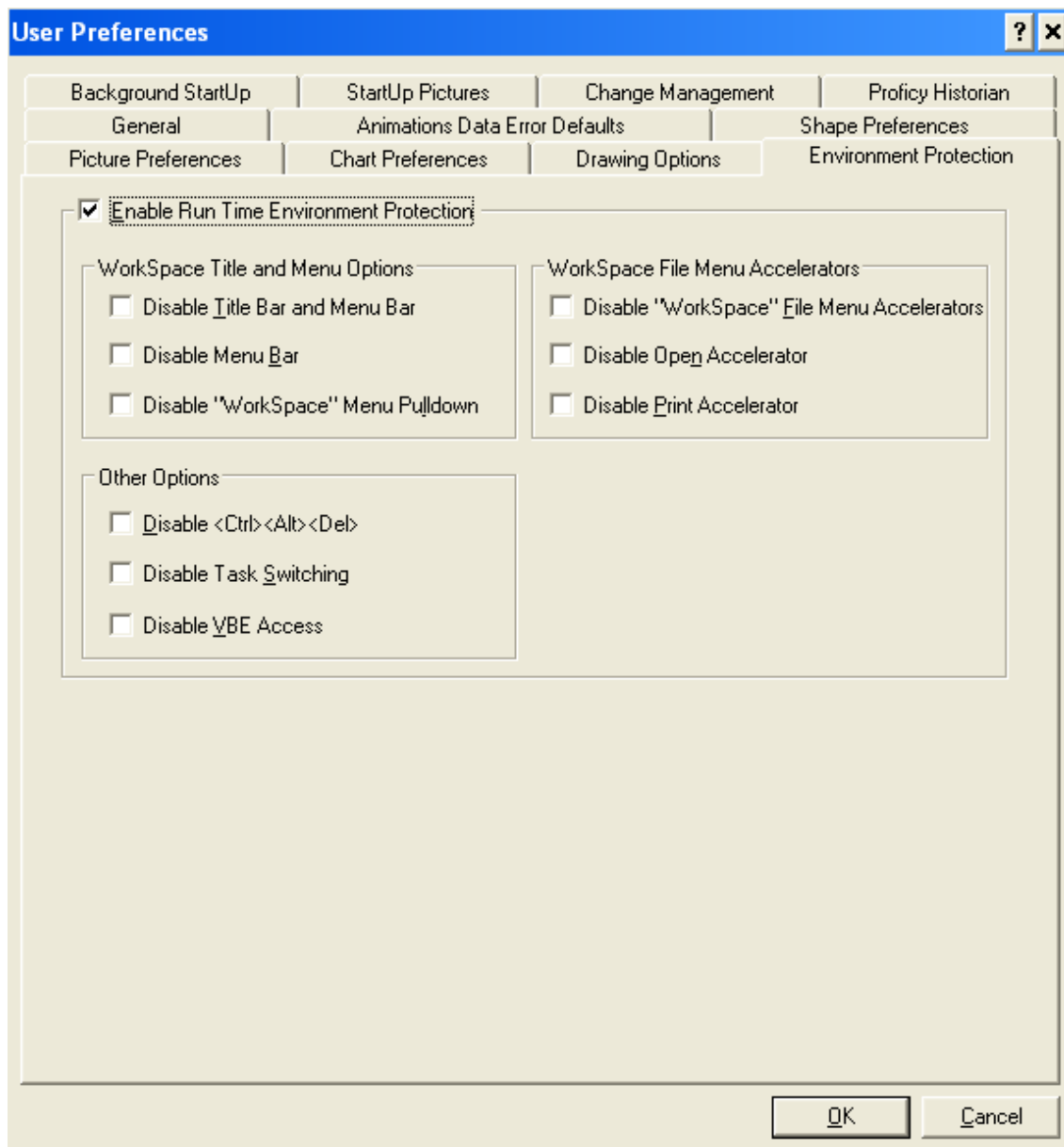


2. Definição de Permissões para Grupos e Usuários

O iFix nos permite bloquear uma série de recursos do Windows, sem a necessidade de uso de ferramentas externas.

Como princípio básico, bloqueia-se tudo e depois se faz a liberação de certos recursos para grupos de usuários ou usuários específicos.

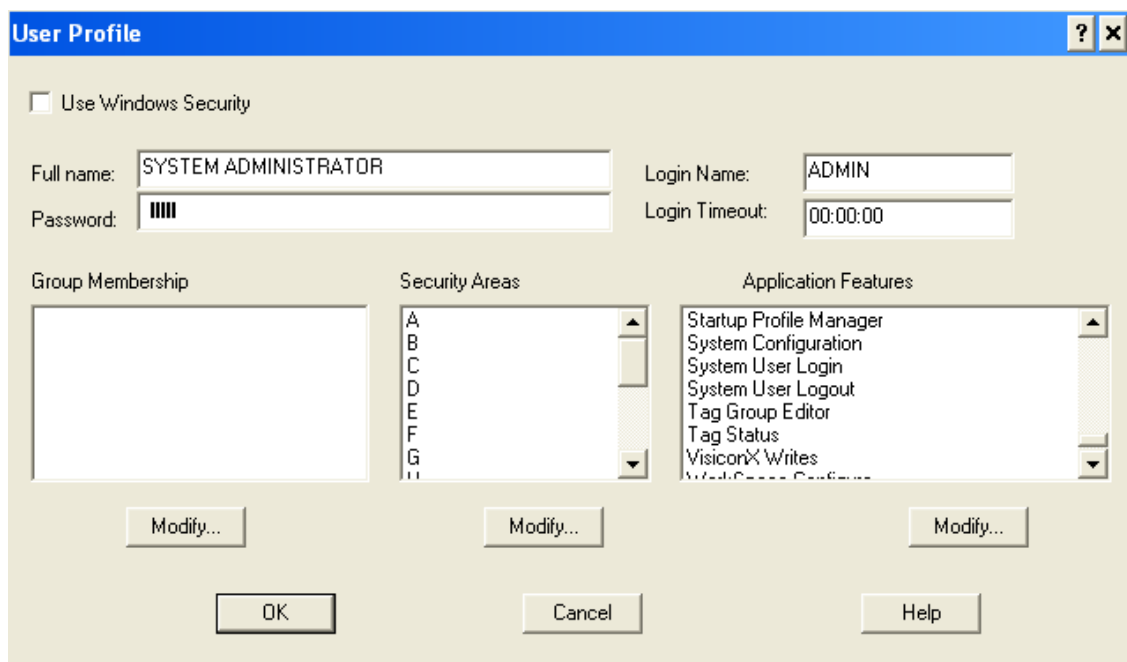
Dentro do Workspace, no menu "Workspace/User Preferences/Environment Protection", têm-se a opção de bloquear diversos tipos de atalho do Windows, como Ctrl + Alt + Del, Alt + Tab, Alt + F4, Iniciar do Windows e outros.



Além dos atalhos bloqueados, todos os acessos à configuração de telas, schedules, scripts, receitas, fechamento do iFix e muitos outros recursos passam a ser bloqueados a todos os usuários ou grupos de usuários que não tenham permissão ao recurso específico.

Os usuários podem ser sincronizados com os configurados na segurança do Windows, o que permite o gerenciamento das senhas de acesso e outras configurações em um local único e de forma centralizada.

O acesso às telas da aplicação, bem como a restrição de escrita/atuação em tags do processo também poderão ser limitados através da configuração de áreas de segurança.



The image shows a 'User Profile' dialog box with a blue title bar. It contains several input fields and lists. At the top left is a checkbox 'Use Windows Security'. Below it are fields for 'Full name' (containing 'SYSTEM ADMINISTRATOR'), 'Login Name' (containing 'ADMIN'), 'Password' (masked with '||||'), and 'Login Timeout' (containing '00:00:00'). There are three main sections: 'Group Membership' with an empty list box, 'Security Areas' with a list containing letters A through H, and 'Application Features' with a list containing 'Startup Profile Manager', 'System Configuration', 'System User Login', 'System User Logout', 'Tag Group Editor', 'Tag Status', 'VisiconX Writes', and 'WebServer Configuration'. Each of these three sections has a 'Modify...' button below it. At the bottom of the dialog are 'OK', 'Cancel', and 'Help' buttons.

3. Assinatura Eletrônica

Compatível com a norma 21CFR Part11, o opcional de assinatura eletrônica do iFix permite que todas as ações realizadas pelos usuários em modo de execução (data, hora, nome do usuário e ação realizada) sejam armazenadas nos registros de alarmes do sistema ou em banco de dados relacional. O objetivo principal é ter um histórico de todas as atuações realizadas pelos operadores e as liberações permitidas pela supervisão.

A assinatura eletrônica está vinculada aos tags da base de dados e são exigidas em todas as ações onde haja alteração de valor de um tag, inclusive via script. Pode-se configurar somente a assinatura de operação (*Perform Only*) ou operação e supervisão (*Perform and Verify*).

Analog Input

Basic | **Alarms** | Advanced | Proficy Historian

Alarm Extension Fields

Alarm Field 1 :

Alarm Field 2 :

Security Areas

NONE
NONE
NONE

Options

☐ Enable Output

Filter

☐ Use Smoothing

Value :

Startup

☒ On Scan ☒ Auto

☐ Off Scan ☐ Manual

Electronic Signature

The Electronic Signature option must be purchased in order for these parameters to take effect.

Type

☐ None

☐ Perform Only

☒ Perform and Verify

Options

☒ Allow Continuous Use

☐ Exempt Alarm Acknowledgement

Unsigned Writes

☐ Accept

☐ Log

☒ Reject

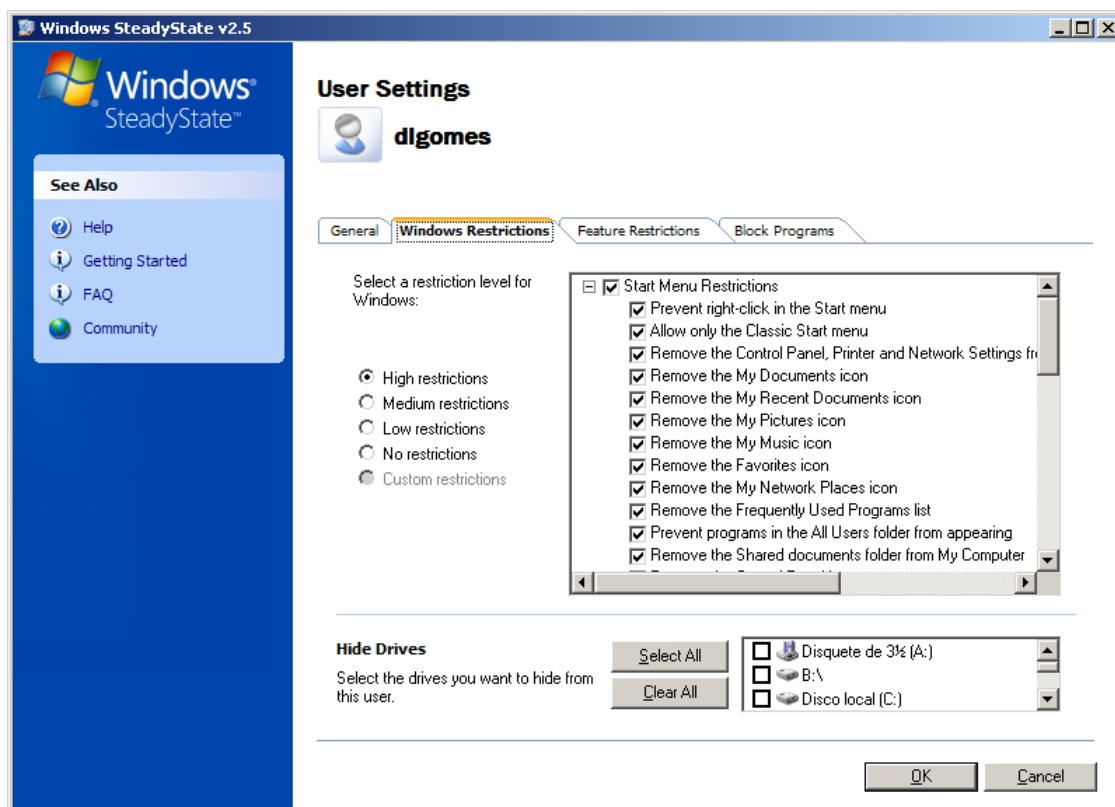
Save Cancel Help

Outros Níveis de Segurança

Quando há servidores de domínio controlando as permissões de usuário através do *Active Directory*, os acessos de usuários a aplicativos ficam centralizados nesse serviço.

Para outros casos, a Microsoft disponibiliza a ferramenta *SteadyState* que permite a configuração de diversas restrições e bloqueios através de sua interface de configuração simples e intuitiva.

Esses bloqueios vão desde programas específicos até acesso a unidades de disco, direitos de clique com o botão direito do mouse na barra de tarefas do Windows, ou mesmo escrita em porta USB.



Uso de Firewall

O uso do *Firewall* é permitido, desde que as portas usadas pelo sistema sejam liberadas.

A porta utilizada pelo iFix é a 2010, porém, caso a empresa use outros meios de comunicação que não seja a cliente/servidor padrão, a liberação de outras portas pode ser necessária.

Antivírus

Não existe restrição quanto ao uso/tipo de antivírus. A única recomendação é que o antivírus esteja desabilitado durante a instalação dos softwares da GE Fanuc.

Muitos clientes utilizam, em especial, os antivírus da Symantec e da McAfee e não existem relatos de problemas com nossos produtos.

Em todo caso, é sempre recomendado o uso das exceções para as pastas do sistema para evitar o reconhecimento de um arquivo ou serviço, essencial para o funcionamento do produto, como vírus.

Para quem trabalha com o driver OPC ou ABR, junto ao RSLinx, para comunicação com dispositivos da Rockwell, existem alguns relatos de situações específicas com antivírus. Maiores informações em <http://support.rockwellautomation.com>.

Aquarius Software

Rua Silva, 110 – 9º andar - Bela Vista, São Paulo – SP
marketing@aquarius.com.br - www.aquarius.com.br

Usuários do Windows

O iFix funciona, sem necessidade de configurações extras, com usuários do Windows membros dos grupos "Power Users" e "Administrators".

Porém, no Windows Vista, os grupos existentes são "Administrators", "Users" e "Guests". Neste caso, é possível configurar direitos avançados para os usuários habilitados em tais grupos.