Segurança no iFix

Por Diogo Gomes

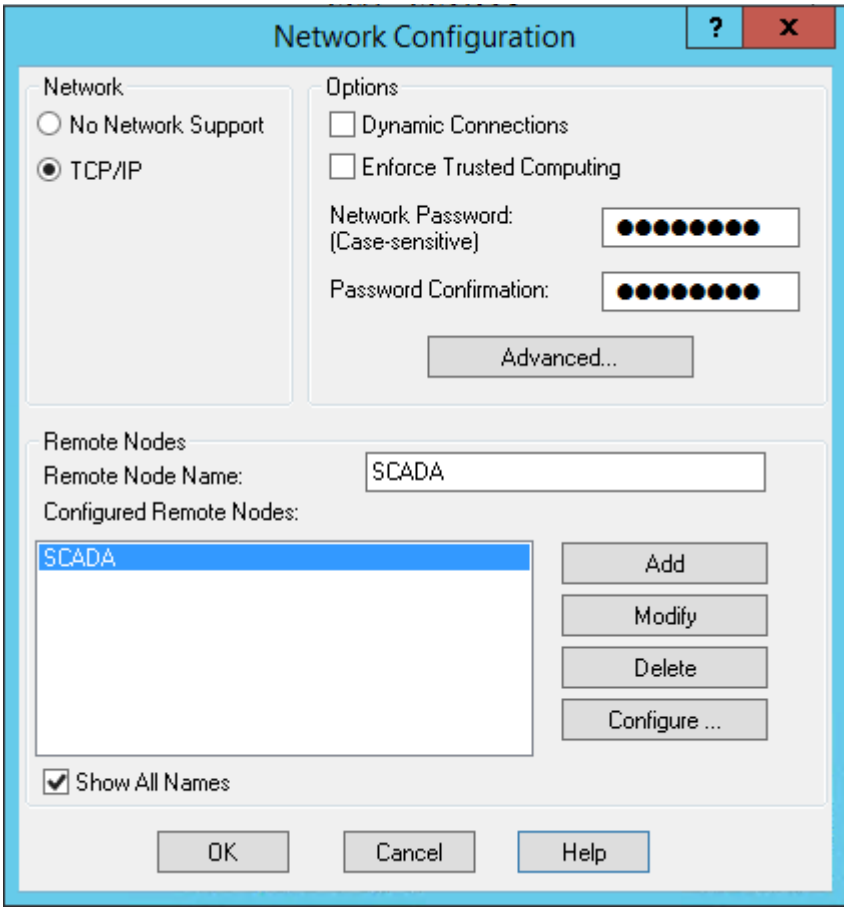
Revisado por Rafael Borges 15/05/2019

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” e depois o campo “Password Confirmation”, 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.

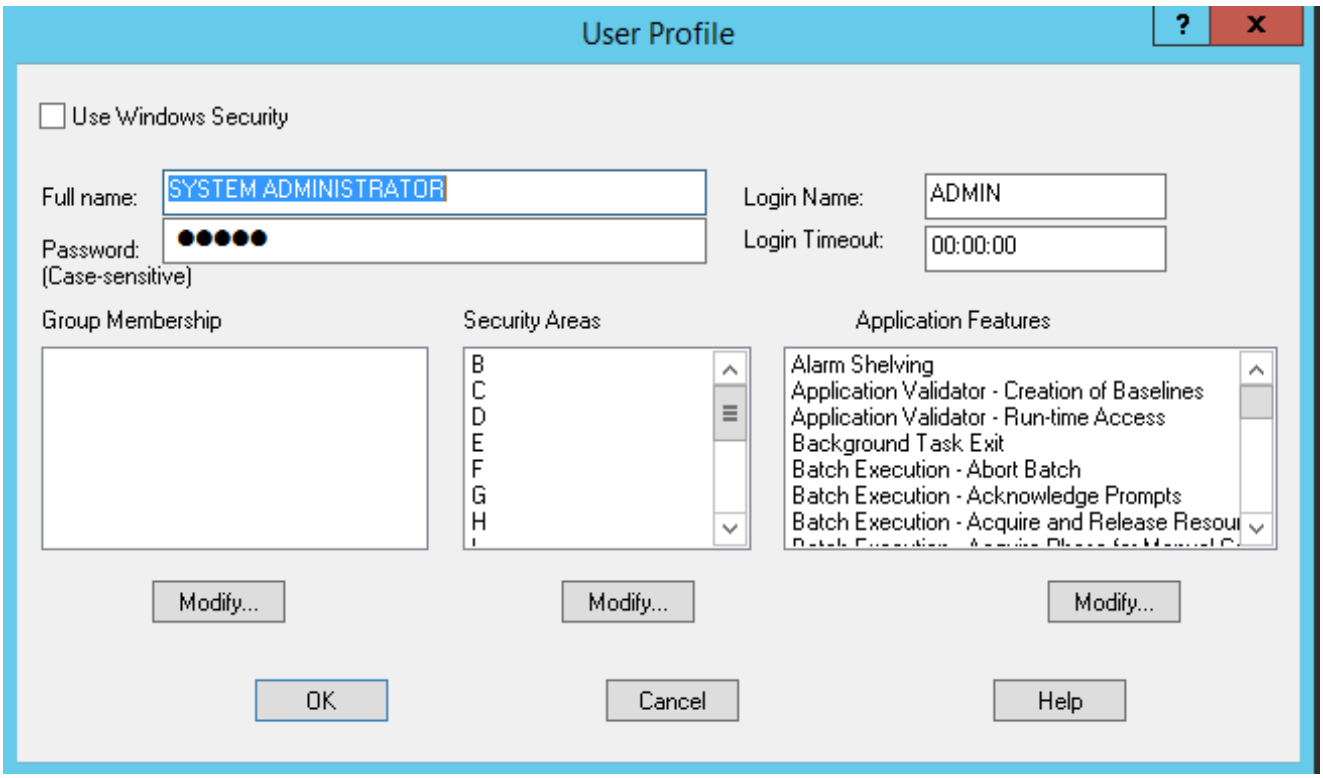
Como princípio básico, bloqueia-se tudo e depois se faz a liberação de certos recursos para grupos de usuários ou usuários específicos.

Dentro do Workspace, no menu “Workspace/User Preferences/Enviroment 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.

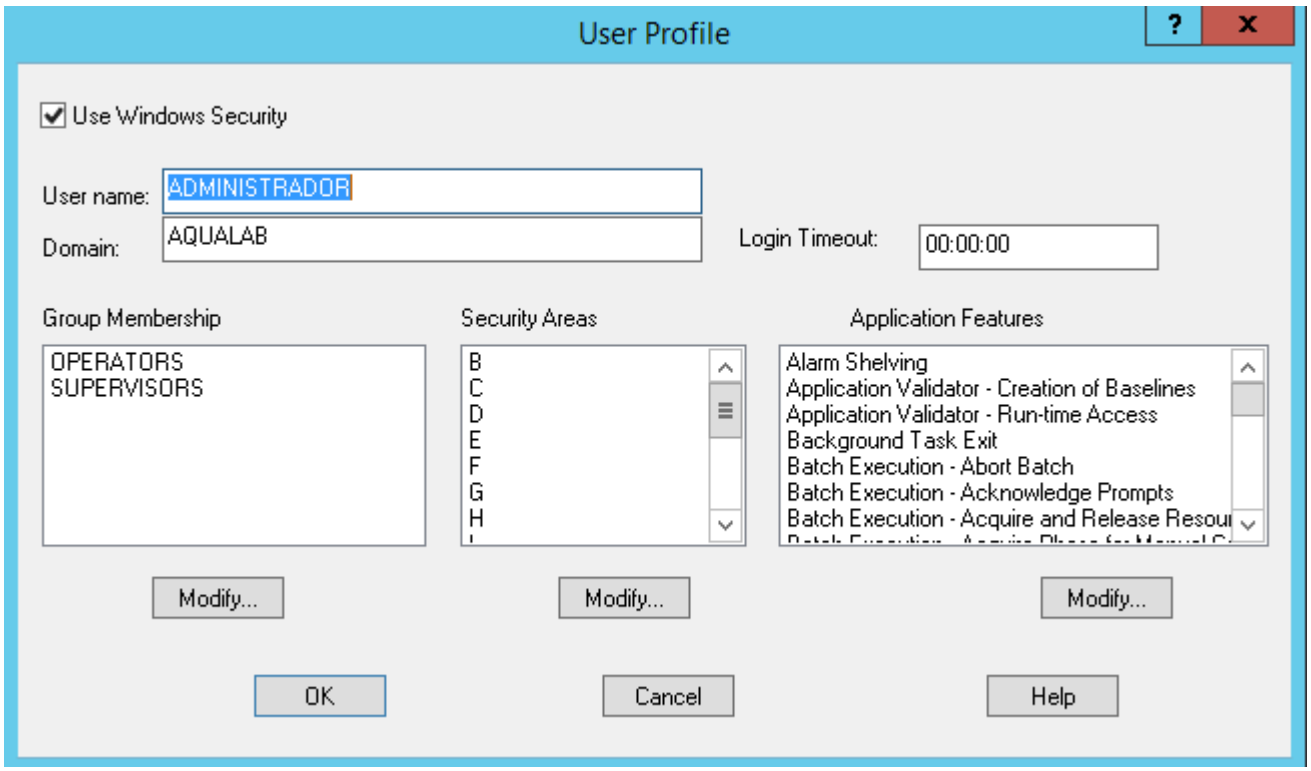
Além dos atalhos bloqueados, todos os acessos à configuração de telas, schedules, scripts, receitas, fechamento do iFix e muitos outros recursos passam a ser bloqueados a todos os usuários ou grupos de usuários que não tenham permissão ao recurso específico.

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.



Habilitando o campo “Use Windows Security” permitirá que o iFix utilize as informações de acesso de um usuário configurado em um controlador de domínio:



Pode-se também limitar o tempo de acesso de um usuário específico preenchendo o campo “Login Timeout”.

NOTA: O campo “Login Timeout” atende o formato “hh:mm:ss”

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 as 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).

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.

Uso de Firewal

O uso do Firewal 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.

Muitos clientes utilizam, em especial, os antivírus da Symantec e da McAfees 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 especificas com antivírus. Maiores informações em http://support.rockwellautomation.com.

Usuários do Windows

O iFix funciona, sem necessidade de configurações extras, com usuários do Windows membro do grupo “Administrators”.

Recomenda-se que durante a instalação e configuração do iFix se utilize o usuário Administrador local.

Última atualização: 16/05/2019