[Autenticação Kerberos](http://confluence.neomind.com.br:8400/pages/viewpage.action?pageId=11534341)

Criar Usuário no ad para integração:

Ex: Kerberos

Configurar SPN:

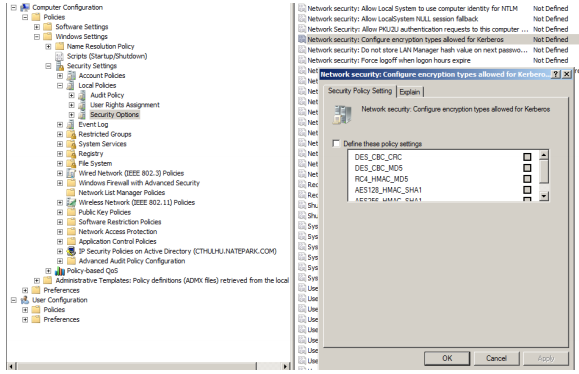
setspn.exe -A HTTP/SERVIDORAD.DOMINIO kerberos  
setspn.exe -A HTTP/SERVIDORAD kerberos

setspn.exe -A HTTP/SERVIDORFUSION.DOMINIO kerberos  
setspn.exe -A HTTP/SERVIDORFUSION kerberos

Politica de Segurança:

TRADUZIR(OBSERVAÇÃO TEMOS QUE ATIVAR TUDO)

In Active Directory environments, the Kerberos etypes can be configured in Group Policy in the following location: Computer Configuration\Policies\Windows Settings\Security Settings\Local Policies\Security Options\Network security: Configure encryption types allowed for Kerberos. If left undefined, which is the default setting, Active Directory will use the highest­strength algorithm. Also note that the DES encryption types have been deprecated in Server 2008 and higher. If legacy Kerberos systems require these, you must define a policy and link it to your domain.



In Active Directory, also check the user’s settings in the Account tab for the following values: ­ Use Kerberos DES encryption types for this account ­ This account supports Kerberos AES 128 bit encryption. ­ This account supports Kerberos AES 256 bit encryption. If in a mixed environment with Domain Controllers running Windows 2000/2003 and DCs running 2008+, enabling AES on the account may cause issues if a user’s TGT session keys are generated with AES and the user attempts to use these session keys for Service Tickets generated on Windows 2000/2003 DCs. Additionally, DES encryption types were deprecated with Windows 2008, so if account principals are configured to use DES, you must either: 1) enable DES via Group Policy as described above; or 2) disable DES on the account options.

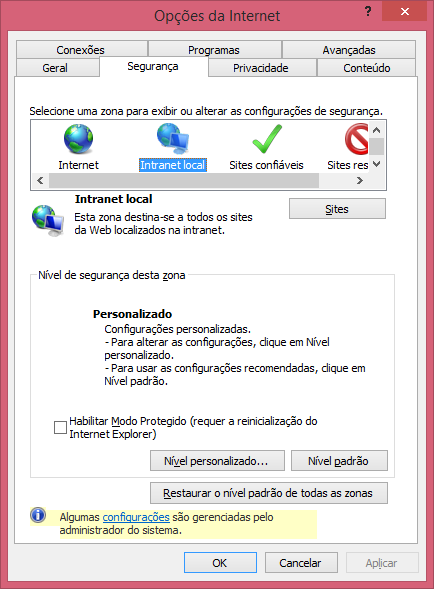
Todos usuários deverão ter habilitados a criptografia de comunicação.



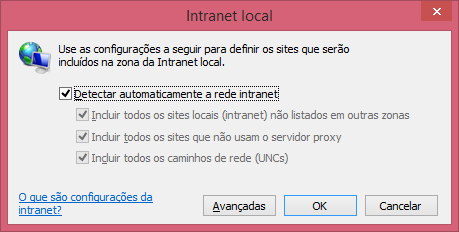
Configuração Navegadores:

IE

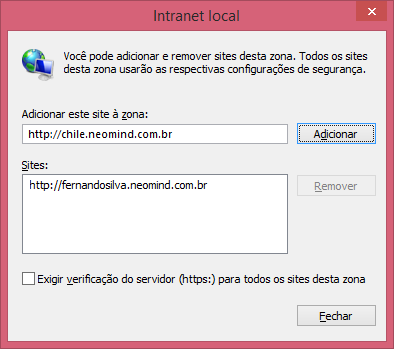
Ir em Opções de Internet:



Abrir a guia Segurança e ir em Intreanet Local / Sites, e marcar as seguintes opções:



Ir em Avançadas: e adicionar o servidor do Fusion como zona confiável ex:



Ir em Opções da Internet / Avançadas e marcar a opção: Habilitar a Autenticação Integrada do Windows

