Configurar a rede Wireless unificada para a autenticação contra o base de dados eDirectory de Novell

Índice

Introdução

No espaço da educação K-12, houve uma necessidade crescente de autenticar usuários Wireless através das contas criadas dentro de Novell eDirectory. Devido à natureza distribuída do ambiente K-12, as escolas individuais não puderam ter os recursos para colocar um servidor Radius em cada local nem fazem elas desejam as despesas gerais adicionais de configurar estes servidores Radius. A única maneira de realizar isto é usando o LDAP para comunicar-se entre o controlador do Wireless LAN (WLC) e um servidor ldap. Os controladores de LAN do Cisco Wireless apoiam a autenticação de EAP local contra bases de dados LDAP externos tais como o microsoft ative directory. Documentos que deste White Paper Cisco WLC configurou para a autenticação de EAP local contra o eDirectory de Novell permitido como um servidor ldap FULL-caracterizado. Uma advertência a notar – os clientes testados usavam o utilitário de desktop do Cisco Aironet para executar a autenticação do 802.1x. Novell atualmente não apoia o 802.1x com seu cliente neste tempo. Em consequência, segundo o cliente, um processo de login de duas fases podia ocorrer. Note estas referências:

Indicação do 802.1x de Novell

“Atualmente, devem entrar duas vezes. Quando o cliente Novell é instalado, um usuário deve entrar usando a caixa de verificação da estação de trabalho somente no diálogo do login inicial para permitir a autenticação de usuário do 802.1x quando o desktop é inicializado, e então devem entrar à rede Novell usando “a utilidade do início de uma sessão N vermelho”. Isto é referido como um início de uma sessão de duas fases.”

Uma alternativa da “ao início de uma sessão estação de trabalho somente” é configurar o cliente Novell para usar “Novell inicial Login=Off” nos ajustes avançados do início de uma sessão (o

padrão é “Novell inicial Login=On”). Para mais informação, refira a autenticação do 802.1x e o cliente Novell para Windows .

Os clientes da terceira parte tais como o cliente de Meetinghouse Aeigs (Cisco Secure Services Client) um parceiro de tecnologia de Novell não podem exigir um início de uma sessão dobro. Para mais informação, refira a ÉGIDE SecureConnect .

Uma outra ação alternativa viável para o cliente Novell é ter a máquina (ou o usuário) autentica (802.1x) ao WLAN antes de Novell GINA que está sendo executada.

Testar uma solução para o único sinal sobre com o cliente Novell e o 802.1x é além do alcance deste White Paper.

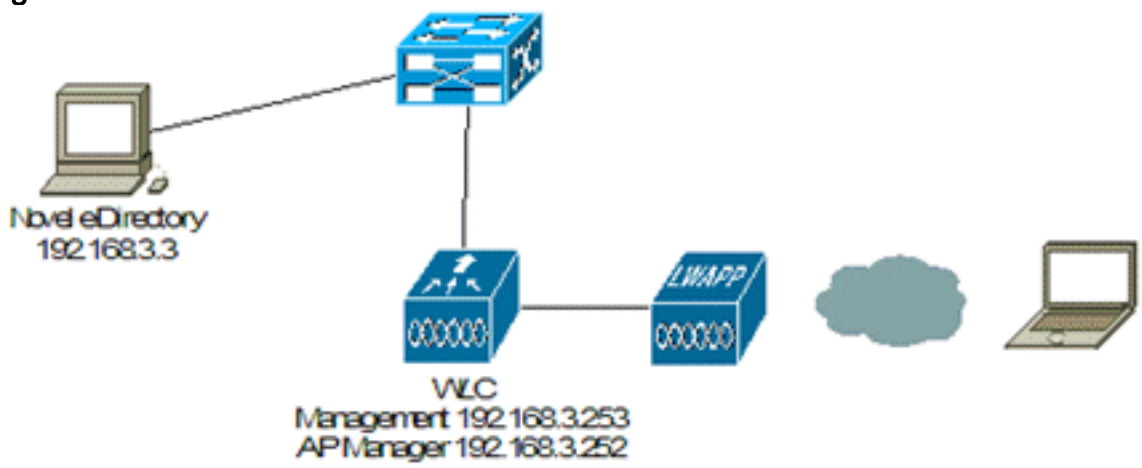
Topologia testada

Solução testada

- Controlador de LAN do Cisco Wireless com software de 6.0.188.0
- Cisco Aironet LWAPP AP 1242AG
- Windows XP com utilitário de desktop 4.4 do Cisco Aironet
- Windows Server 2003 com Novell 8.8,5 eDirectory
- Novell ConsoleOne 1.3.6h (utilitário de gerenciamento eDirectory)

Topologia de rede

Figura 1



Dispositivo	Endereço IP	Máscara de sub-rede	Gateway padrão
Novell eDirectory	192.168.3.3	255.255.255.0	192.168.3.254
Switch de camada 3	192.168.3.254	255.255.255.0	-
AP	Atribuído através do DHCP do interruptor L3	255.255.255.0	192.168.3.254

Relação do gerente da interface de gerenciamento WLC AP WLC	192.168.3.253 192.168.3.252	255.255.255.0	192.168.3.254

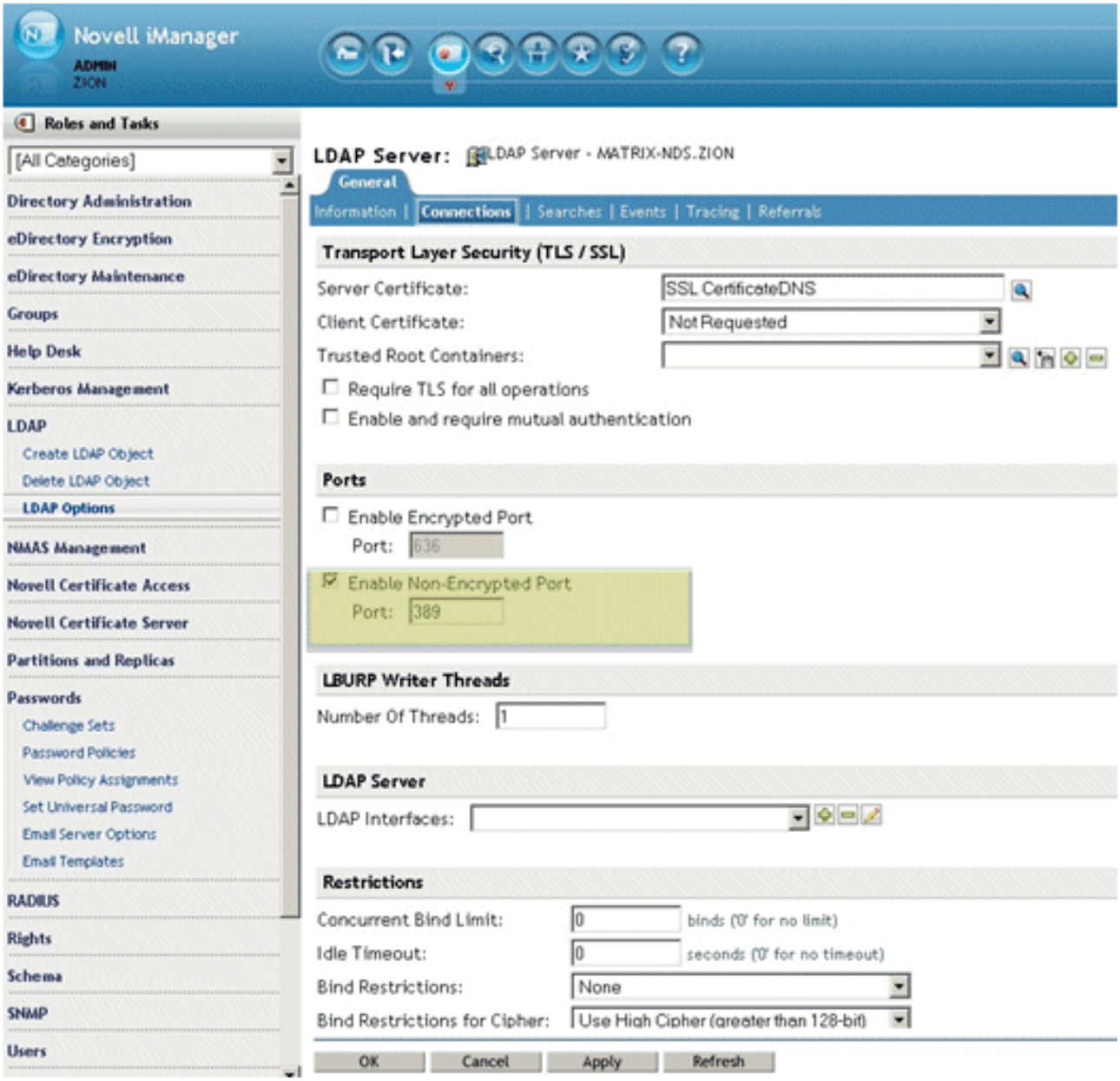
Configuração

Configuração eDirectory de Novell

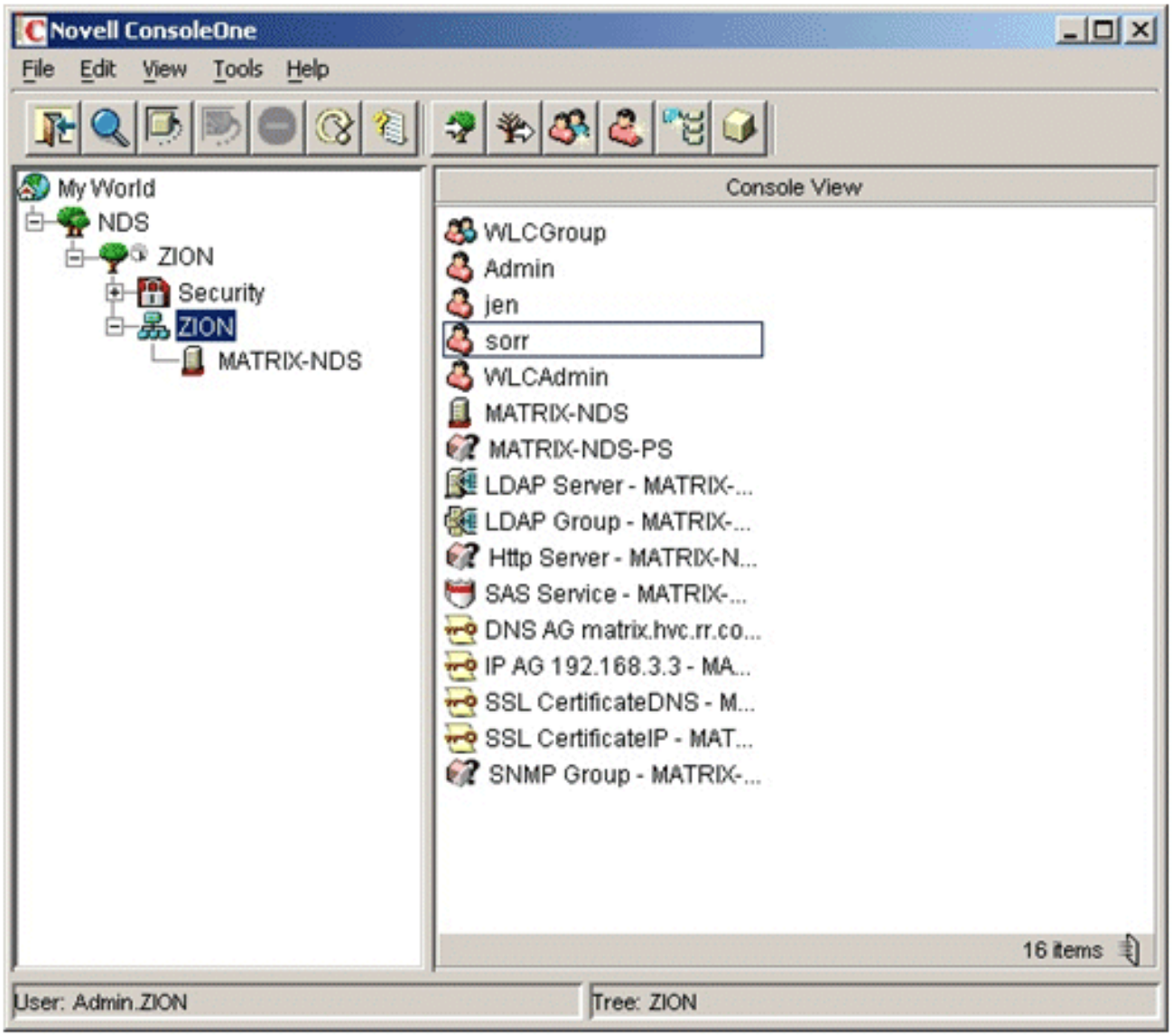
A instalação e a configuração eDirectory completas de Novell são além do alcance deste White Paper. Novell eDirectory deve ser instalado assim como os componentes correspondentes LDAP.

Os parâmetros de configuração chaves exigidos são que a senha simples deve ser permitida para as contas de usuário e o LDAP autenticado deve ser configurado. Usar o TLS para o LDAP foi apoiada nas versões anterior do código WLC (4.2); contudo, o LDAP seguro é apoiado já não no software do controlador de WLAN de Cisco.

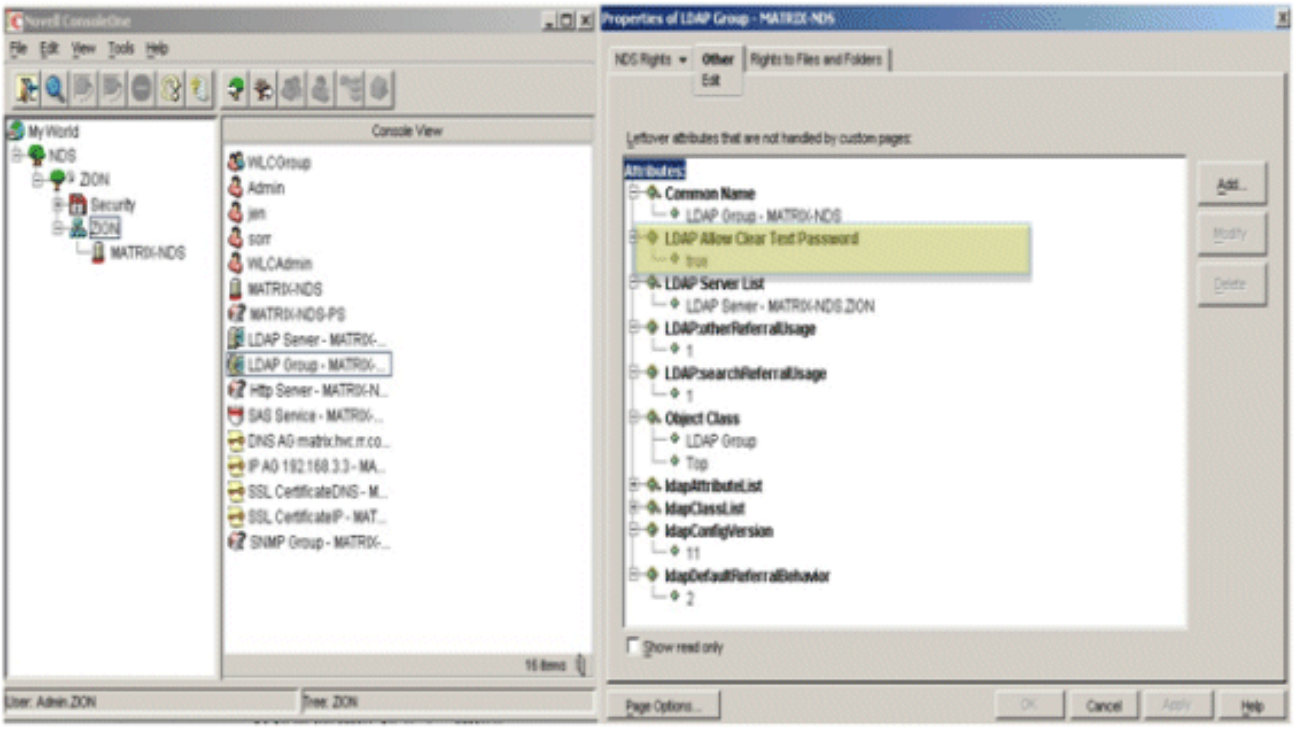
1. Ao configurar a parcela do servidor ldap de eDirectory, certifique-se de que as portas NON-cifradas LDAP (389) estão permitidas. Veja figura 2 do aplicativo do iManager de Novell.**Figura 2**



2. Durante a instalação eDirectory, pedi-lo-á a estrutura de árvore ou o Domain Name, etc. Se eDirectory é instalado já, o ConsoleOne de Novell (figura 3) é uma ferramenta fácil por que para ver a estrutura eDirectory. É crítico encontrar o que os esquemas apropriados são ao tentar estabelecer uma comunicação ao WLC. Você deve igualmente ter uma conta criada que permita que o WLC execute um ligamento autenticado ao servidor ldap. Para a simplicidade, neste caso, a conta admin eDirecotry de Novell é usada para o ligamento autenticado.**Figura 3**

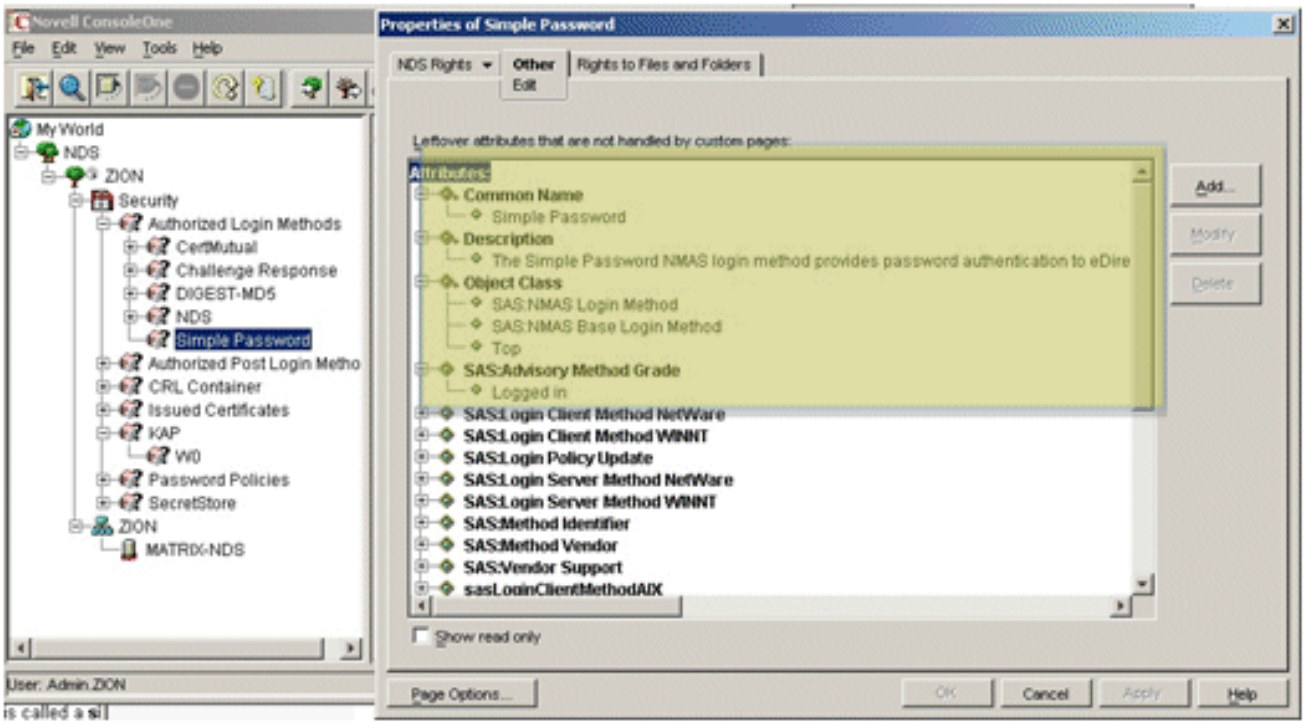


3. Use ConsoleOne a fim verificar que o grupo LDAP permite **senhas de texto sem formatação**.Figura 4



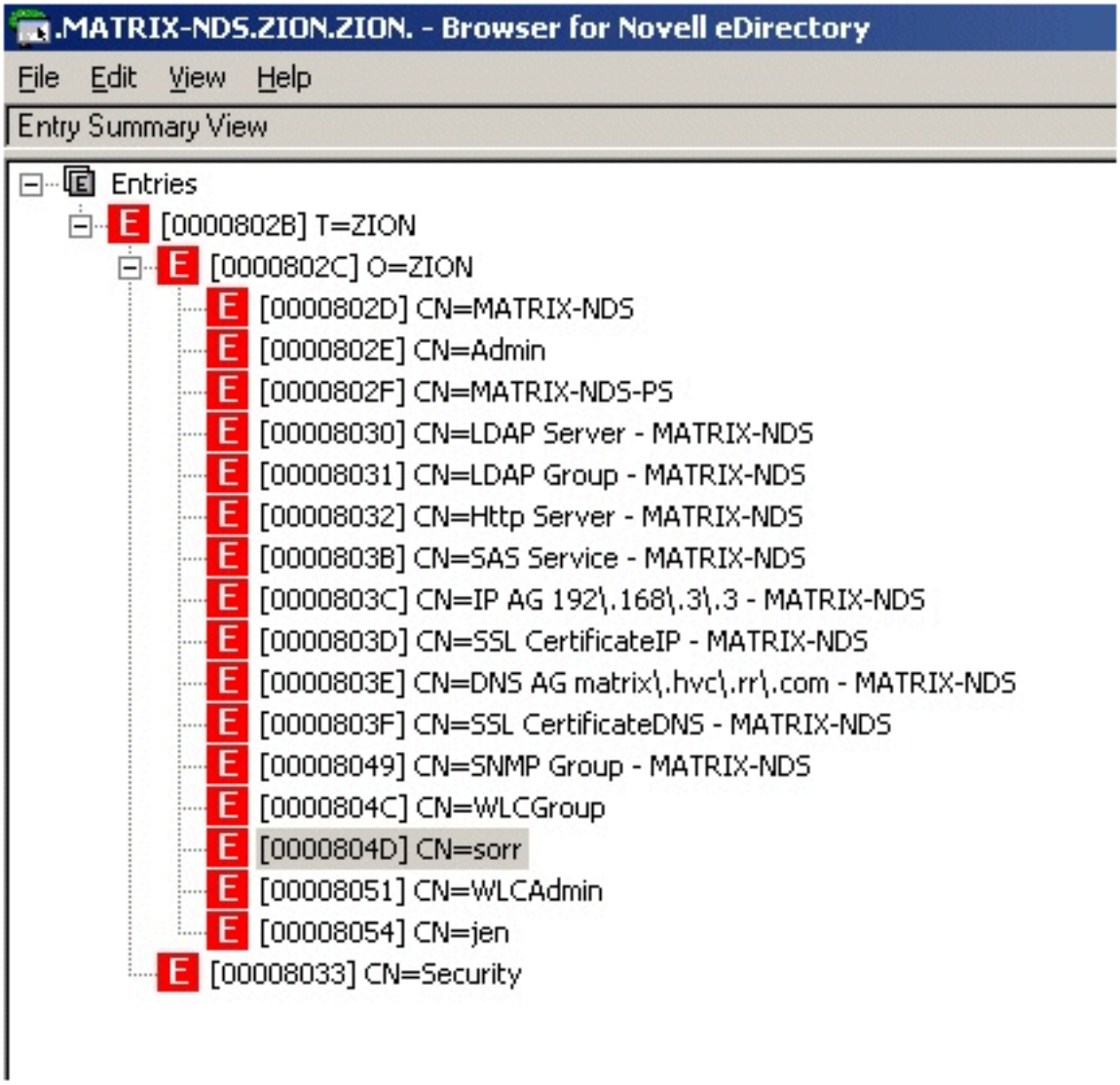
4. Verifique que sob o OU, configurações de segurança que a **senha simples** está

permitida.**Figura 5**



Uma outra ferramenta útil por que ver a estrutura eDirectory de Novell é o navegador incluiu com a instalação padrão.

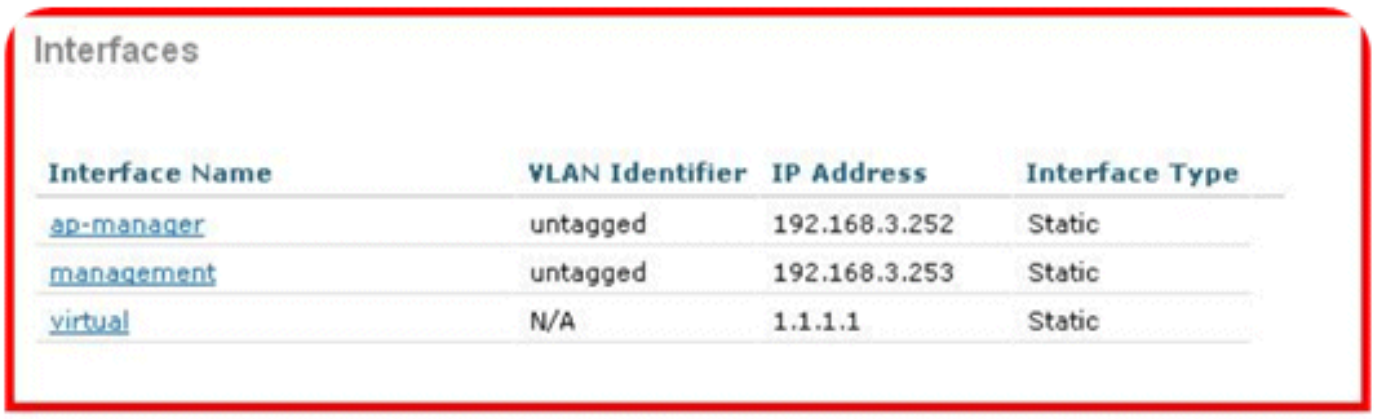
Figura 6



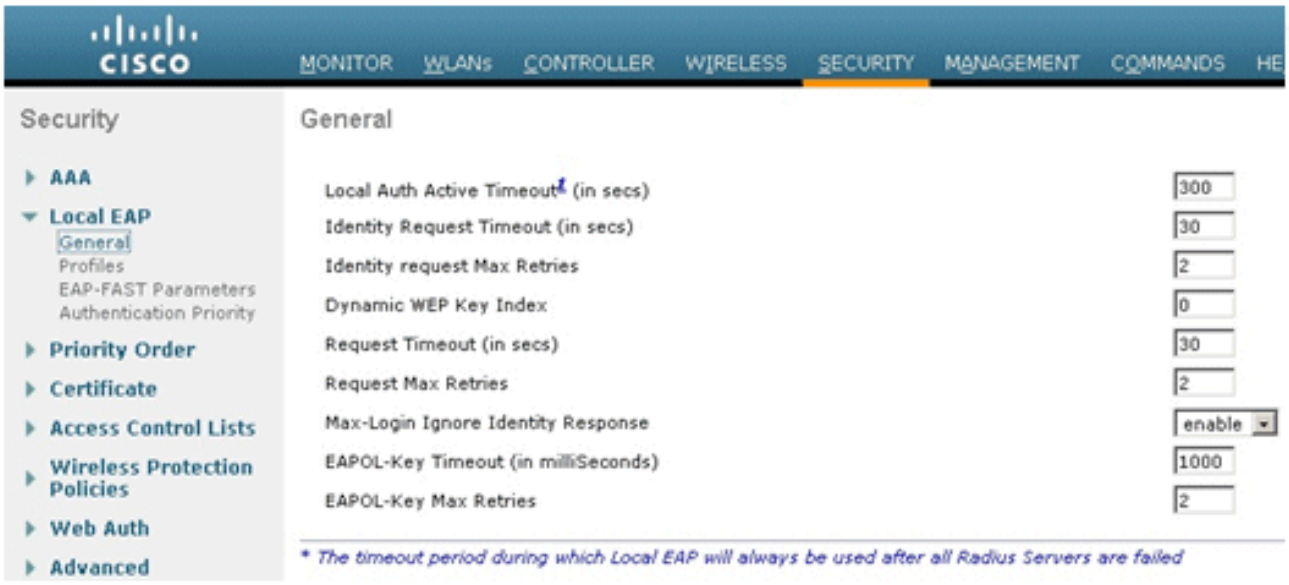
Configuração de WLC

Consulte para figurar 1 para a topologia física da rede de teste. O WLC usado neste teste foi configurado de acordo com a prática padrão com o gerenciador AP e as interfaces de gerenciamento na mesma sub-rede e o sem etiqueta de uma perspectiva VLAN.

Figura 7



1. Configurar a autenticação de EAP local: **Segurança > local EAP > general**.Os padrões padrão não foram mudados.**Figura 8**



2. Crie um perfil novo do Local EAP: **Segurança > local EAP > perfis**.Para este caso de teste, o nome de perfil local EAP escolhido era eDirectory. Os métodos de autenticação escolhidos eram PULO, EAP-FAST e PEAP; contudo, somente o PEAP foi testado neste documento.**Figura 9**

Quando você configura a autenticação de EAP local para o PEAP, você deve ter um certificado instalado no WLC. Neste caso, para propósitos testando, o certificado instalado fábrica de Cisco foi usado; contudo, um certificado fornecida do cliente pode igualmente ser instalado. Os certificados do lado do cliente não são exigidos para o uso do PEAP-GTC, mas podem ser permitidos para o método interno PEAP se for necessário.**Figura 10**

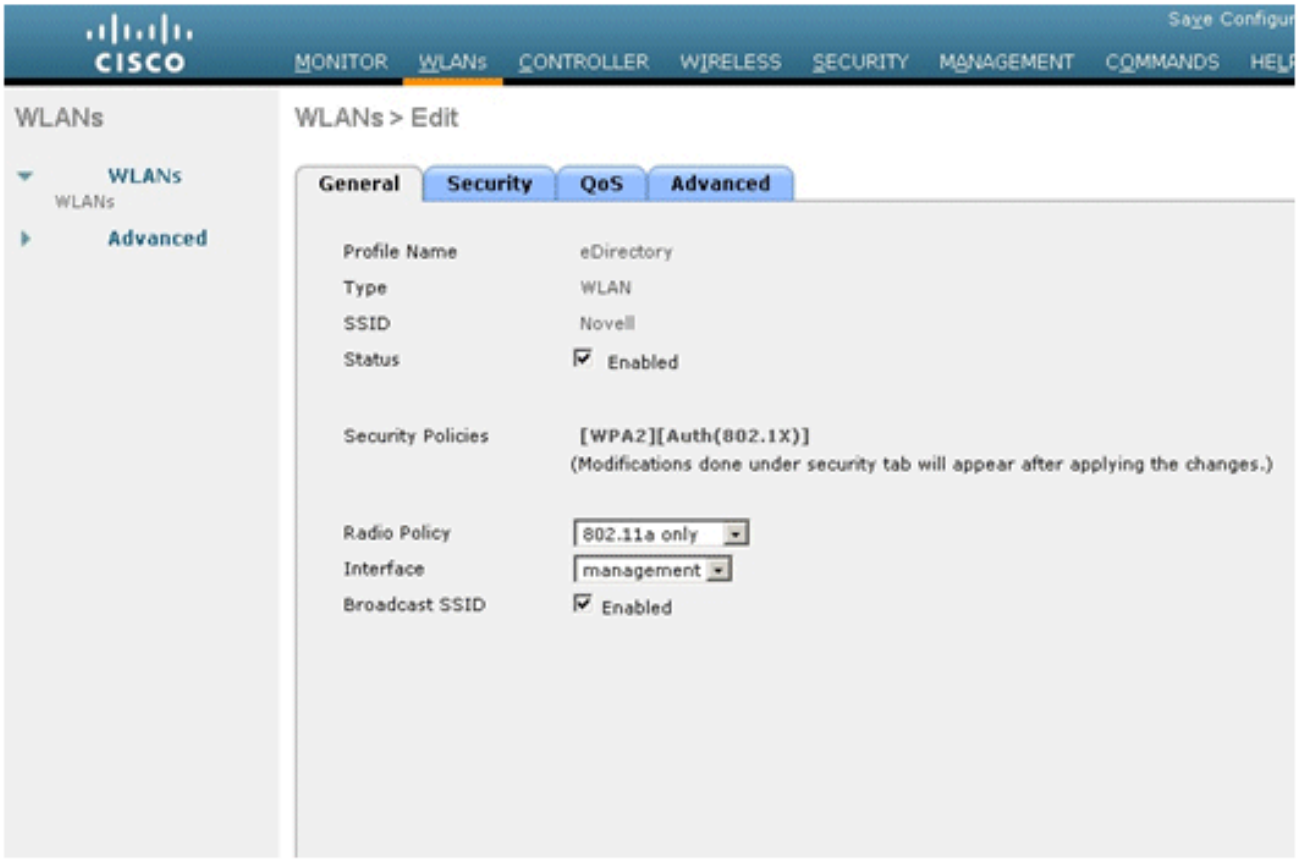
3. Ajuste a prioridade da autenticação para o LDAP: **Segurança > local EAP > prioridade da autenticação**.**Figura 11**

4. Adicionar o servidor ldap ao WLC: **Segurança > AAA > LDAP**.**Figura 12**

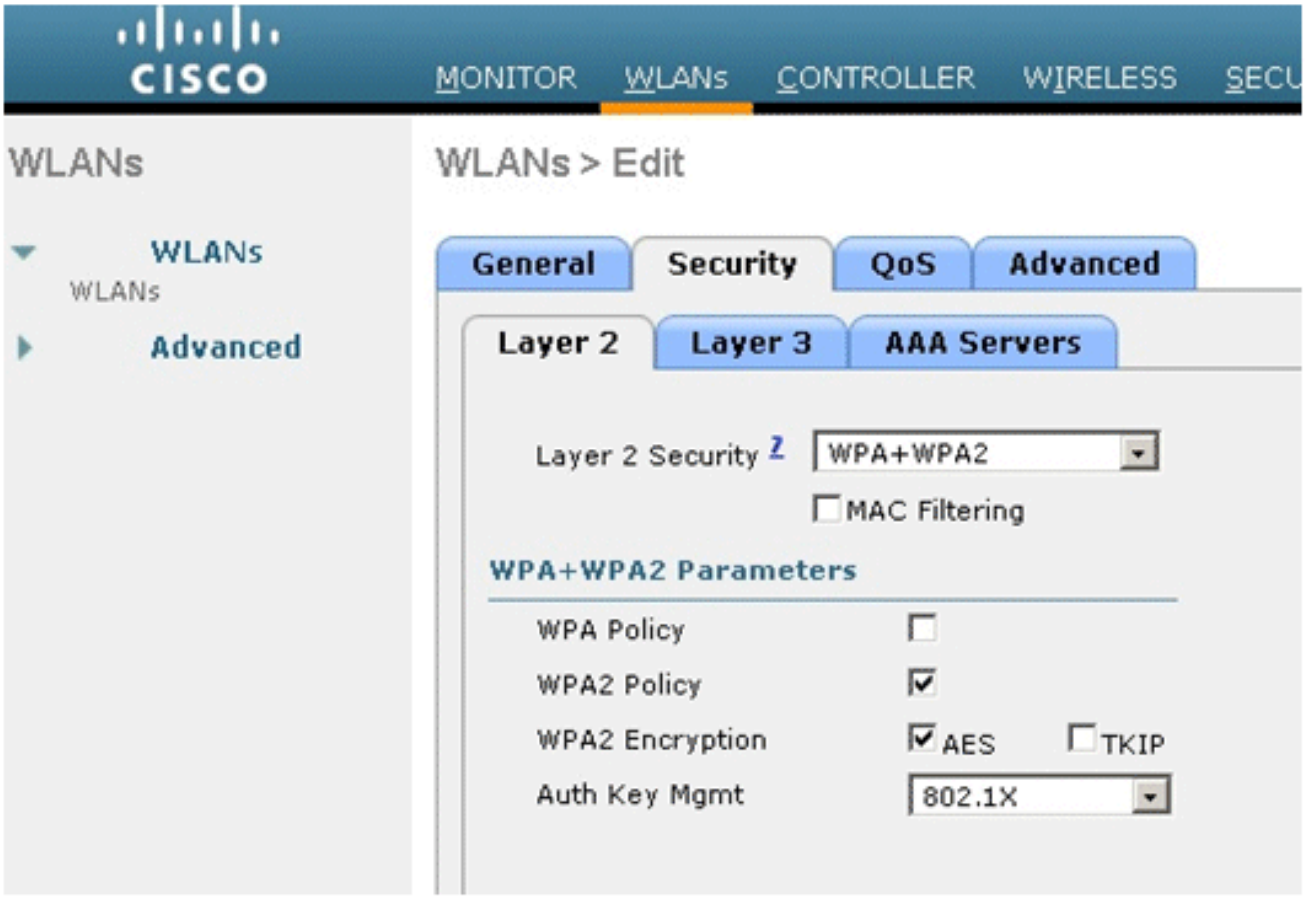
5. Configurar o WLC para usar eDirecotry novo (veja figura 13):Escolha **autenticado** para o método simples do ligamento.Incorpore o username do ligamento. Esta é a conta que foi criada dentro a eDirectory que será usado para que o WLC ligue a eDirectory.**Nota:** Certifique-se de que você incorpora os atributos do diretório correto para o username. Para este caso de teste, o “cn=Admin, o=ZION” foi usado.Incorpore a senha do ligamento. Esta é a senha para a conta de usuário do ligamento.Incorpore a base do usuário DN. Este é o Domain Name onde as contas de usuário Wireless são encontradas. No caso de teste, os usuários foram ficados situados na raiz do DN (o=Zion). Se são aninhados dentro de outros grupos/organizações, acorrente-os junto com uma vírgula (por exemplo, “o=ZION, o=WLCUser”).Incorpore o atributo de usuário. Este é o Common Name (CN) (veja a figura 6).Tipo de objeto do usuário – Isto é ajustado ao *usuário*.**Figura 13**

6. Crie o WLAN que você quer os clientes eDirectory de Novell se usar. Para este caso de teste, o nome de perfil WLAN é *eDirectory* e o SSID é *Novell* (veja figura 14).**Figura 14**

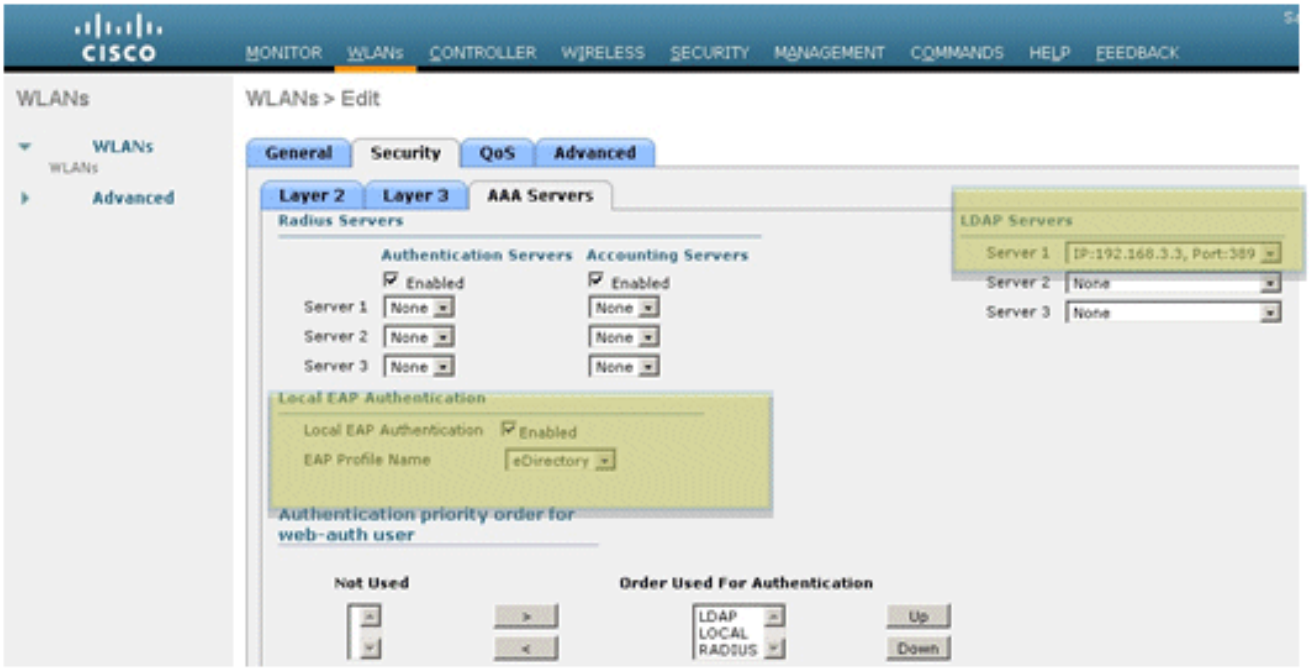
7. Permita o WLAN e aplique a política de rádio apropriada e conecte-a. Para este caso de teste, Novell SSID foi permitido somente para a rede 802.11a e amarrado à interface de gerenciamento.**Figura 15**



8. Configurar as configurações de segurança apropriadas da camada 2. Para este caso de teste, a Segurança WPA+WPA2, a política WPA2, a criptografia de AES, e o 802.1x para o gerenciamento chave foram selecionados.**Figura 16**



9. Para terminar a configuração local da autenticação de EAP, configurar o WLAN para a autenticação de EAP local usando o servidor ldap:Escolha a **autenticação de EAP local permitida** e aplique o perfil criado EAP (**eDirectory**).Sob os servidores ldap, escolha o endereço IP de Um ou Mais Servidores Cisco ICM NT do server eDirectory configurado (**192.168.3.3**).**Figura 17**



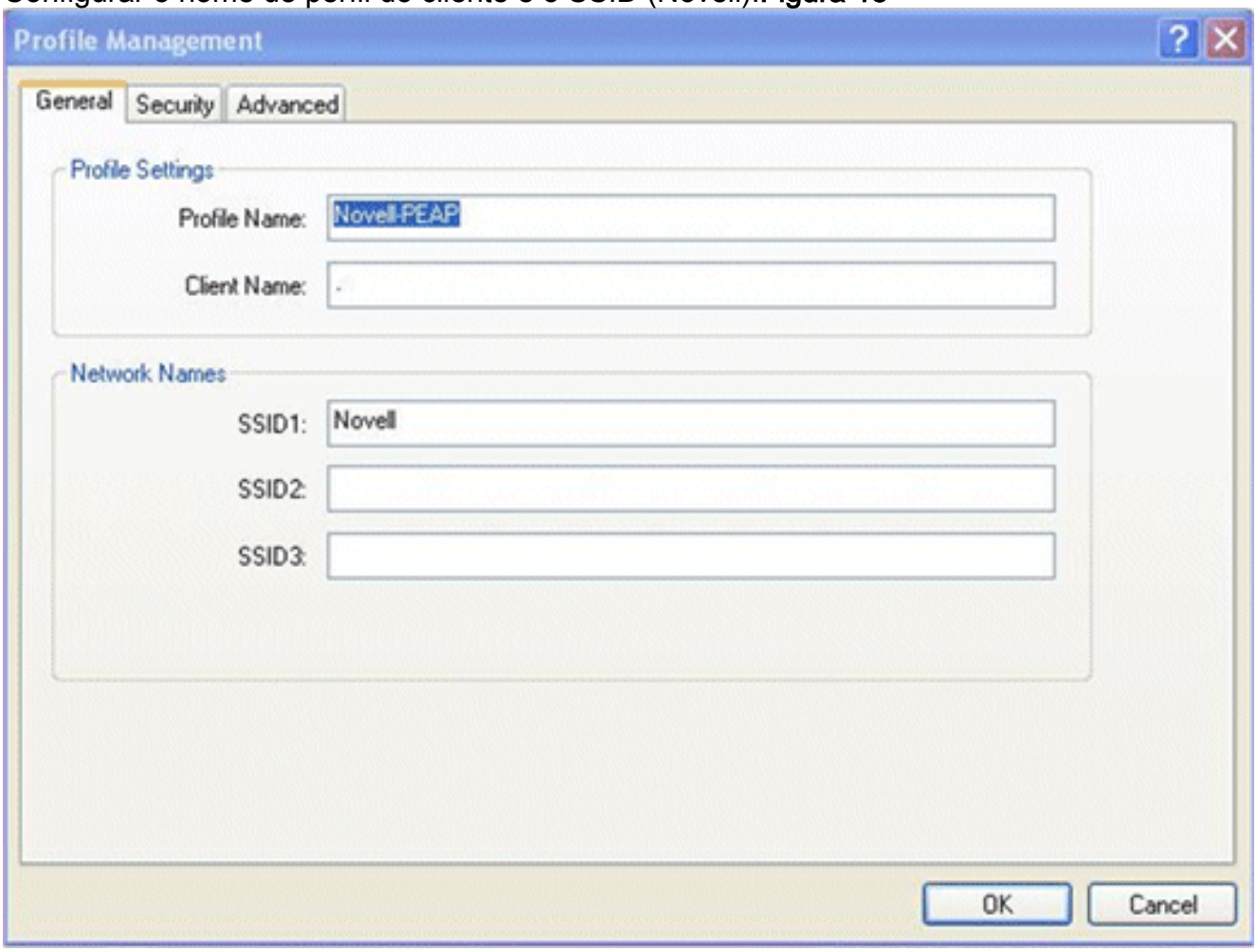
Configuração do Cliente

O PEAP-GTC é o requisito de autenticação atual para a maioria das escolas K-12. O WLC não apoia o MSCHAPv2 para a autenticação de EAP local. Em consequência, você deve escolher o

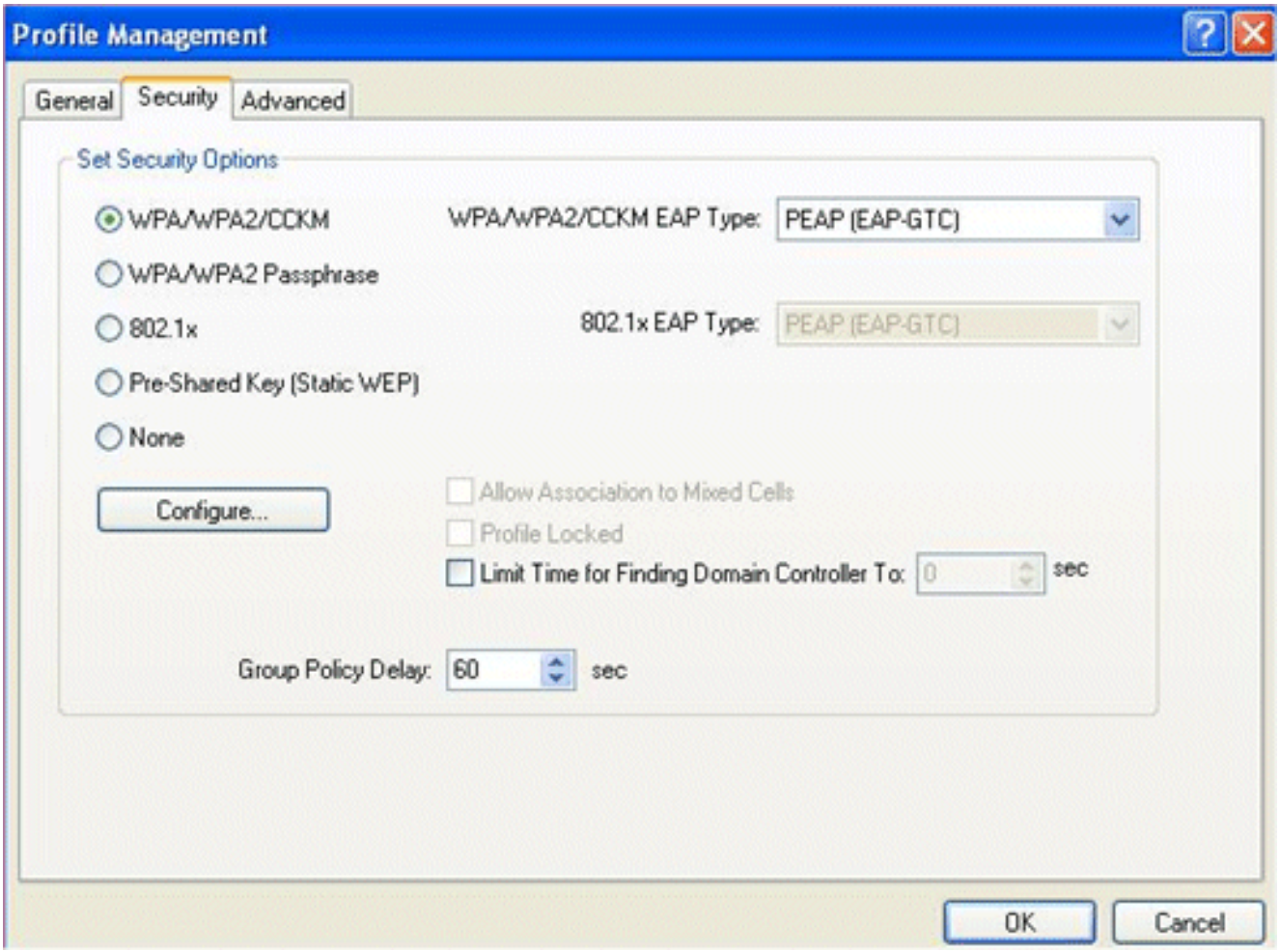
GTC para o tipo da autenticação de EAP no cliente.

As seguintes figuras são um procedimento da configuração do utilitário de desktop do Cisco Aironet para que o PEAP-GTC conecte ao WLAN SSID Novell. As configurações similares são conseguidas com o cliente Microsoft nativo com apoio PEAP-GTC.

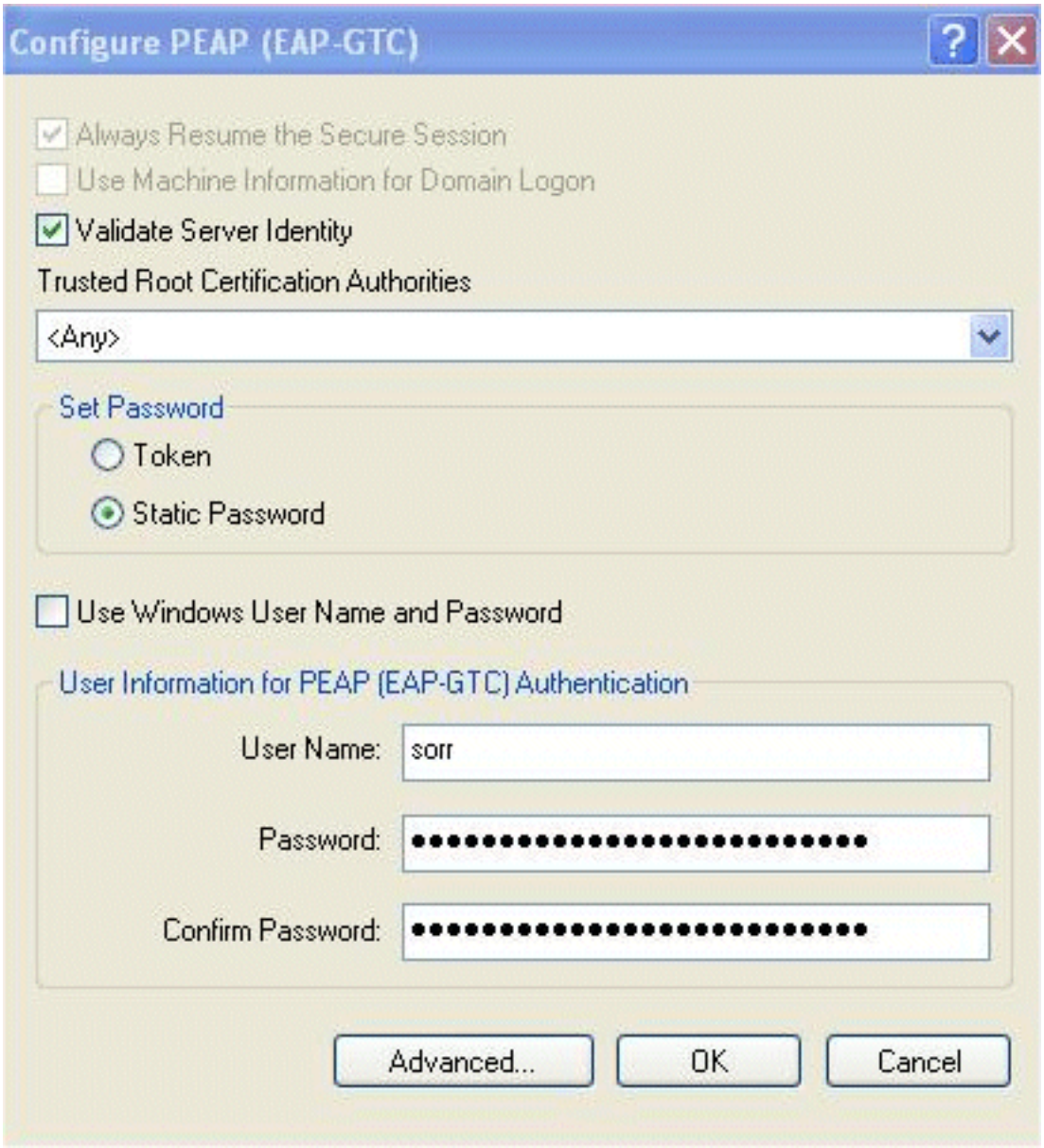
1. Configurar o nome de perfil do cliente e o SSID (Novell).**Figura 18**



2. Escolha **WPA/WPA2/CCKM** para a Segurança e o **PEAP (EAP-GTC)** para o tipo EAP.**Figura 19**



3. Configurar o PEAP-GTC:Escolha **validam a identidade** e a **senha estática do server**.Incorpore o nome de usuário e senha para a conta ou o suplicante alertará para as credenciais no fazer logon.Não entre no esquema do diretório **<ANY>** Novell, como isto não é exigido.**Figura 20**



4. Uma vez que o perfil é terminado, ative-o e o processo de autenticação deve começar.**Figura 21**

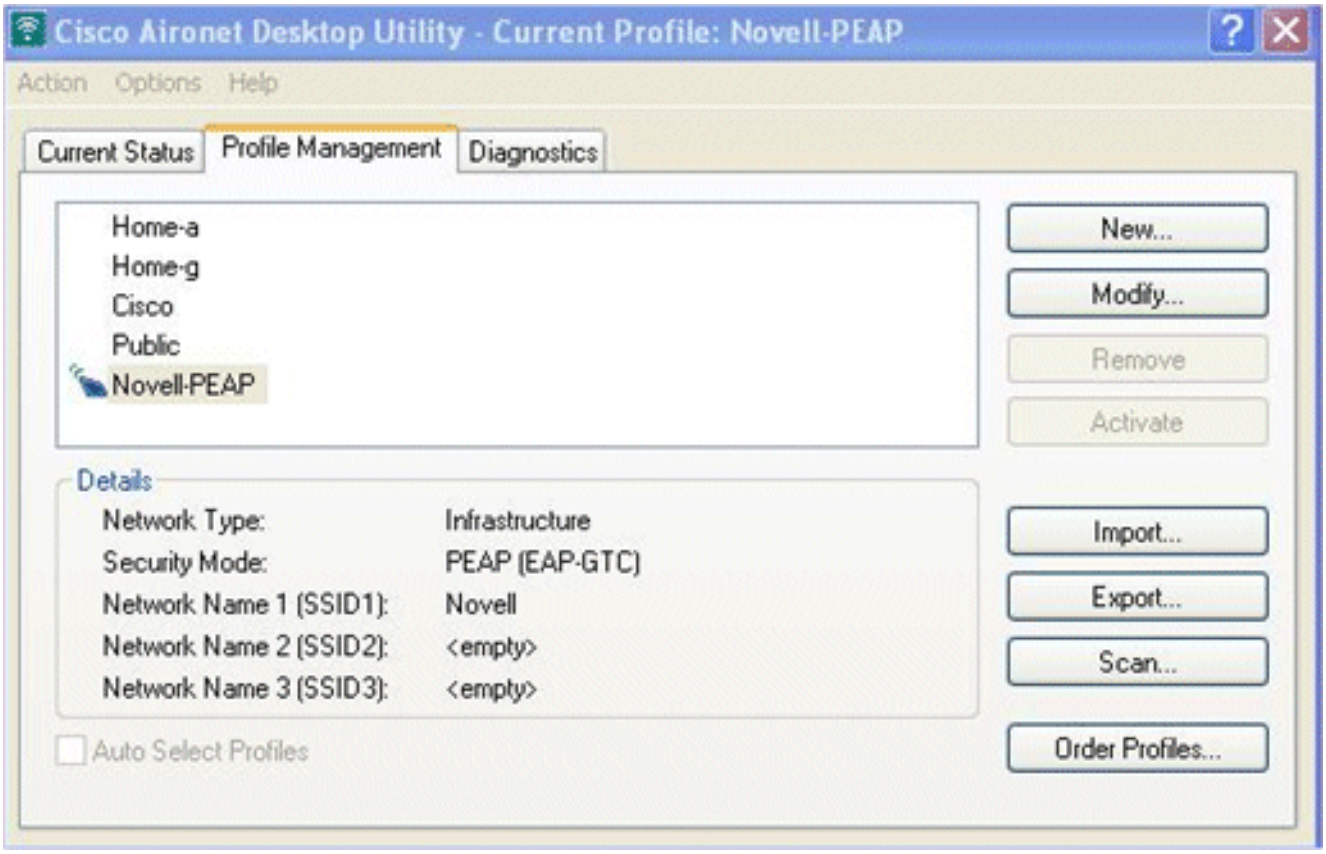
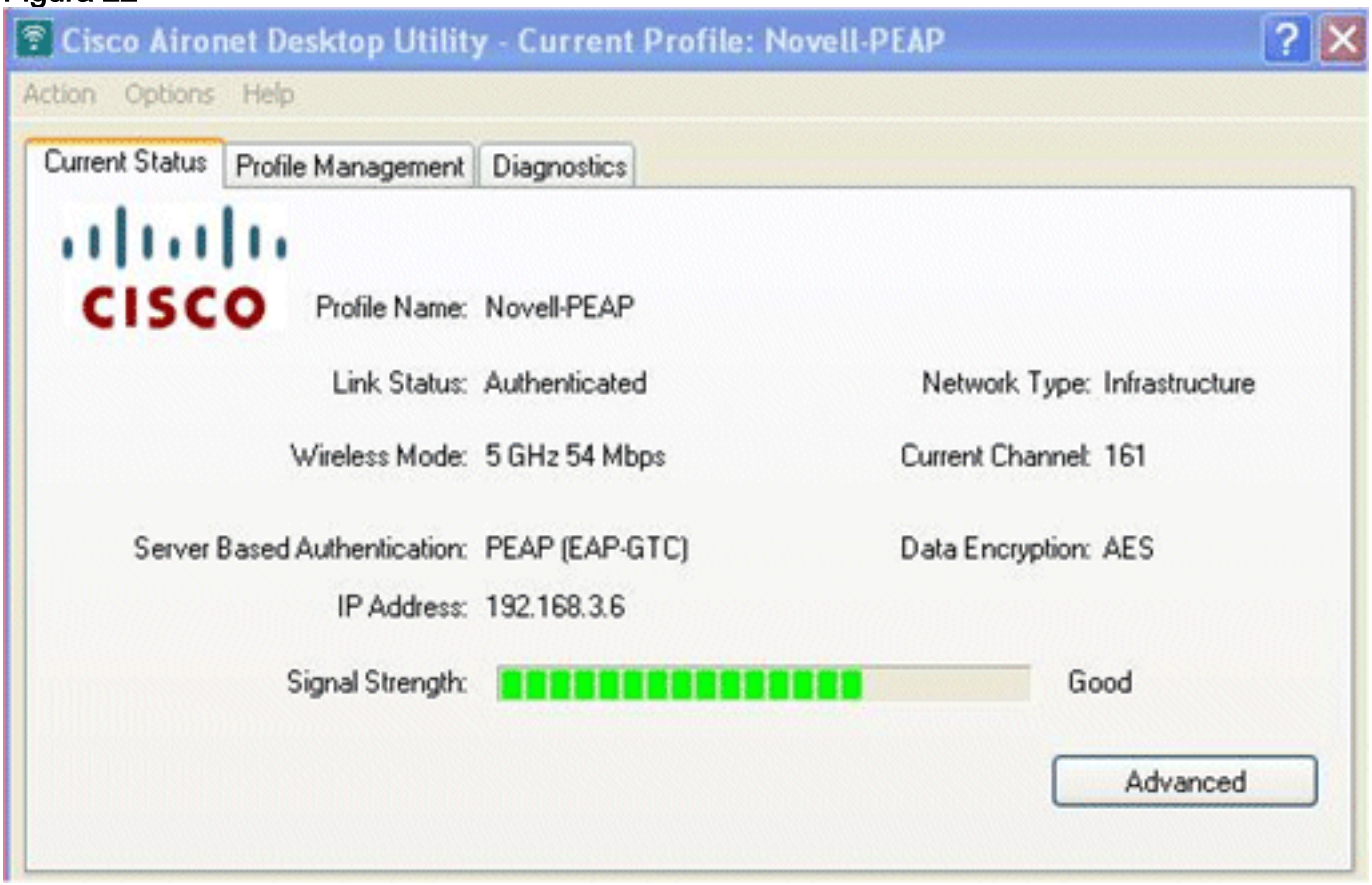


Figura 22 descreve uma associação e uma autenticação bem sucedidas através do PEAP-GTC.

Figura 22

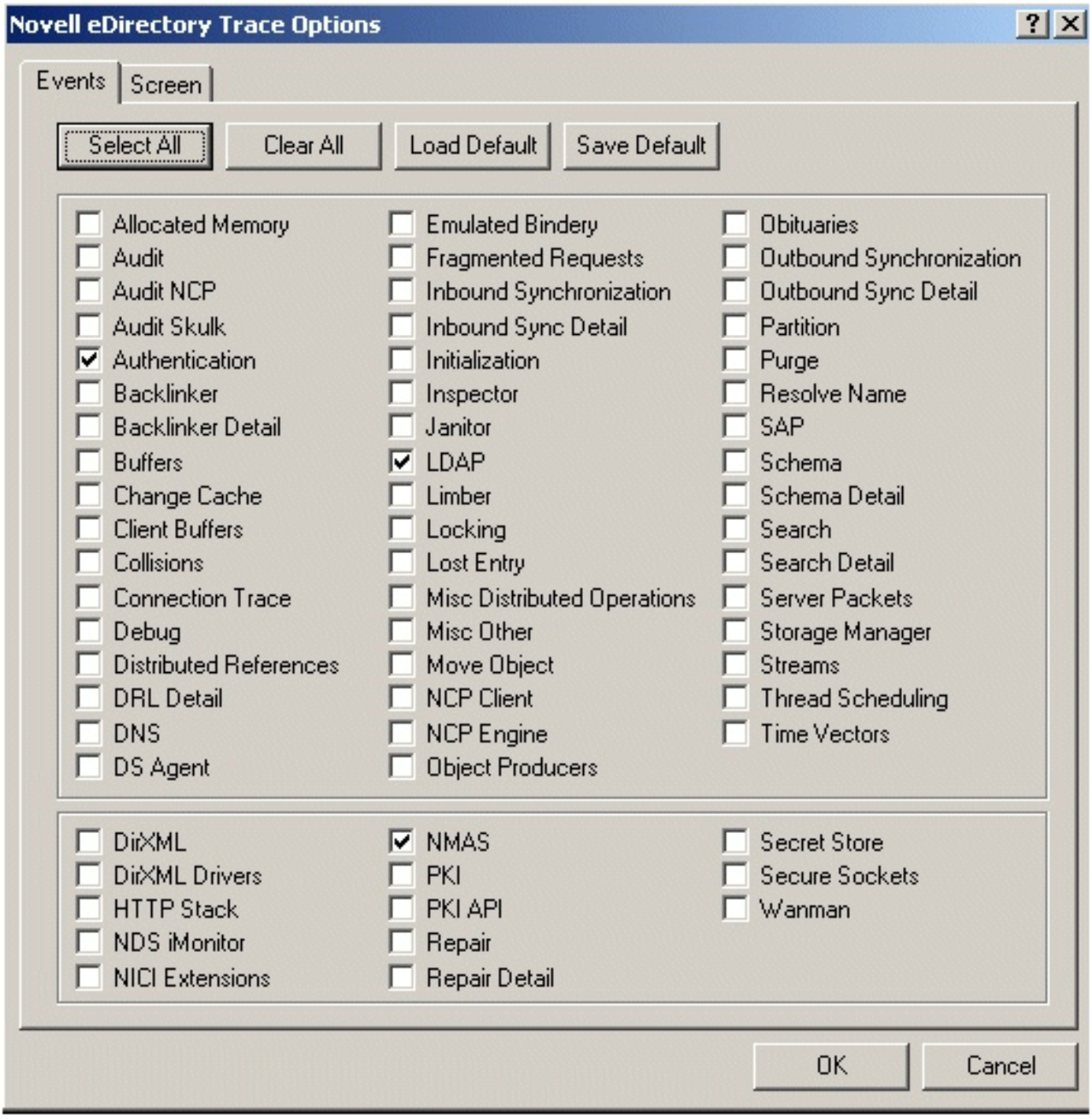


Debugs

Para verificar que você pode executar um LIGAMENTO autenticado assim como a autenticação de usuário, permite estas opções do traço para eDirectory:

- Autenticação
- LDAP
- NMAS

Figura 23



Segundo as indicações debugar, uma resposta bem sucedida da autenticação LDAP é entregada ao controlador do Wireless LAN em 192.168.3.253:

```
LDAP   : (192.168.3.253:36802)(0x0020:0x63) DoSearch on connection
    0x34367d0
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Search request:
      base: "o=ZION"
      scope:2  dereference:0  sizelimit:0  timelimit:5  attrsonly:0
      filter: "(&(objectclass=user)(cn=sorr))"
      attribute: "dn"
      attribute: "userPassword"
```

```
Auth   : Starting SEV calculation for conn 23, entry .sorr.ZION.ZION..
Auth   : 1 GlobalGetSEV.
Auth   : 4 GlobalGetSEV succeeded.
Auth   : SEV calculation complete for conn 23, (0:0 s:ms).
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Sending search result entry
    "cn=sorr,o=ZION" to connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0020:0x63) Sending operation result 0:"":"" to
    connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) DoSearch on connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Search request:
      base: "o=ZION"
      scope:2  dereference:0  sizelimit:0  timelimit:5  attrsonly:0
      filter: "(&(objectclass=user)(cn=sorr))"
      attribute: "dn"
      attribute: "userPassword"
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Sending search result entry
    "cn=sorr,o=ZION" to connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0021:0x63) Sending operation result 0:"":"" to
    connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0022:0x60) DoBind on connection 0x34367d0
LDAP   : (192.168.3.253:36802)(0x0022:0x60) Bind name:cn=sorr,o=ZION, version:3,
    authentication:simple
Auth   : [0000804d] <.sorr.ZION.ZION.> LocalLoginRequest. Error success, conn:
    22.
LDAP   : (192.168.3.253:36802)(0x0022:0x60) Sending operation result 0:"":"" to
    connection 0x34367d0
Auth   : UpdateLoginAttributesThread page 1 processed 1 login in 0 milliseconds
```

Nota: Algumas das linhas no resultado do debug foram envolvido devido às limitações do espaço.

Para assegurar-se de que o WLC esteja fazendo um pedido da autenticação bem sucedida ao server eDirectory, emita estes comandos debug no WLC:

```
debug aaa ldap enable

debug aaa local-auth eap method events enable

debug aaa local-auth db enable
```

Exemplo de saída de uma autenticação bem sucedida:

```
*Dec 23 16:57:04.267: LOCAL_AUTH: (EAP) Sending password verify request profile
    'sorr' to LDAP
*Dec 23 16:57:04.267: AuthenticationRequest: 0xcdb6d54
*Dec 23 16:57:04.267:   Callback.....................................0x84cab60
*Dec 23 16:57:04.267:   protocolType.................................0x00100002
*Dec 23 16:57:04.267:   proxyState...................................
    00:40:96:A6:D6:CB-00:00
*Dec 23 16:57:04.267:   Packet contains 3 AVPs (not shown)
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from LL
*Dec 23 16:57:04.267: EAP-AUTH-EVENT: Waiting for asynchronous reply from method
*Dec 23 16:57:04.267: ldapTask [1] received msg 'REQUEST' (2) in state
    'CONNECTED' (3)
*Dec 23 16:57:04.267: disabled LDAP_OPT_REFERRALS
*Dec 23 16:57:04.267: LDAP_CLIENT: UID Search (base=o=ZION,
    pattern=(&(objectclass=user)(cn=sorr)))
*Dec 23 16:57:04.269: LDAP_CLIENT: ldap_search_ext_s returns 0 85
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned 2 msgs including 0 references
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned msg 1 type 0x64
*Dec 23 16:57:04.269: LDAP_CLIENT: Received 1 attributes in search entry msg
*Dec 23 16:57:04.269: LDAP_CLIENT: Returned msg 2 type 0x65
*Dec 23 16:57:04.269: LDAP_CLIENT : No matched DN
```

```
*Dec 23 16:57:04.269: LDAP_CLIENT : Check result error 0 rc 1013
*Dec 23 16:57:04.269: LDAP_CLIENT: Received no referrals in search result msg
*Dec 23 16:57:04.269: ldapAuthRequest [1] called lcapi_query base="o=ZION"
    type="user" attr="cn" user="sorr" (rc = 0 - Success)
*Dec 23 16:57:04.269: Attempting user bind with username cn=sorr,o=ZION
*Dec 23 16:57:04.273: LDAP ATTR> dn = cn=sorr,o=ZION (size 14)
*Dec 23 16:57:04.273: Handling LDAP response Success
*Dec 23 16:57:04.274: LOCAL_AUTH: Found context matching MAC address - 448
*Dec 23 16:57:04.274: LOCAL_AUTH: (EAP:448) Password verify credential callback
    invoked
*Dec 23 16:57:04.274: eap_gtc.c-TX-AUTH-PAK:
*Dec 23 16:57:04.274: eap_core.c:1484: Code:SUCCESS  ID:0x 8  Length:0x0004
    Type:GTC
*Dec 23 16:57:04.274: EAP-EVENT: Received event 'EAP_METHOD_REPLY' on handle
    0xBB000075
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: Handling asynchronous method response for
    context 0xBB000075
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: EAP method state: Done
*Dec 23 16:57:04.274: EAP-AUTH-EVENT: EAP method decision: Unconditional Success
*Dec 23 16:57:04.274: EAP-EVENT: Sending method directive 'Free Context' on
    handle 0xBB000075
*Dec 23 16:57:04.274: eap_gtc.c-EVENT: Free context
*Dec 23 16:57:04.274: id_manager.c-AUTH-SM: Entry deleted fine id 68000002 -
    id_delete
*Dec 23 16:57:04.274: EAP-EVENT: Sending lower layer event 'EAP_SUCCESS' on
    handle 0xBB000075
*Dec 23 16:57:04.274: peap_inner_method.c-AUTH-EVENT: EAP_SUCCESS from inner
    method GTC
*Dec 23 16:57:04.278: LOCAL_AUTH: EAP: Received an auth request
*Dec 23 16:57:04.278: LOCAL_AUTH: Found context matching MAC address - 448
*Dec 23 16:57:04.278: LOCAL_AUTH: (EAP:448) Sending the Rxd EAP packet (id 9) to
    EAP subsys
*Dec 23 16:57:04.280: LOCAL_AUTH: Found matching context for id - 448
*Dec 23 16:57:04.280: LOCAL_AUTH: (EAP:448) ---> [KEY AVAIL] send_len 64,
    recv_len 64
*Dec 23 16:57:04.280: LOCAL_AUTH: (EAP:448) received keys waiting for success
*Dec 23 16:57:04.280: EAP-EVENT: Sending lower layer event 'EAP_SUCCESS' on
    handle 0xEE000074
*Dec 23 16:57:04.281: LOCAL_AUTH: Found matching context for id - 448
*Dec 23 16:57:04.281: LOCAL_AUTH: (EAP:448) Received success event
*Dec 23 16:57:04.281: LOCAL_AUTH: (EAP:448) Processing keys success
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb [BE-resp] AAA response 'Success'
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb [BE-resp] Returning AAA response
*Dec 23 16:57:04.281: 00:40:96:a6:d6:cb AAA Message 'Success' received for
    mobile 00:40:96:a6:d6:cb
```

Nota: Algumas das linhas na saída foram envolvido devido às limitações do espaço.

Porque mais escolas K-12 adotam a arquitetura de WLAN de Cisco, haverá uma necessidade crescente de apoiar a autenticação de usuário Wireless a Novell eDirectory. Este papel verificou que Cisco WLC pode autenticar usuários contra o base de dados LDAP eDirectory de Novell quando configurado para a autenticação de EAP local. Uma configuração similar pode igualmente ser feita com o Cisco Secure ACS que autentica usuários a Novell eDirectory. As investigações adicionais devem ser feitas para o único sinal sobre com outros clientes de WLAN tais como a configuração zero do Cisco Secure Services Client e do Microsoft Windows.

Informações Relacionadas

- Autenticação de EAP local no controlador do Wireless LAN com exemplo de configuração EAP-FAST e do servidor ldap

- Exemplo de configuração de servidor local unificado da rede Wireless EAP
- Autenticação EAP-FAST com exemplo de configuração dos controladores e do servidor de raio externo do Wireless LAN
- Suporte Técnico e Documentação - Cisco Systems