Configure Unified Wireless Network for Authentication Against Novell's eDirectory Database

Document ID: 112137

Contents

Introduction
Tested Topology
Solution Tested
Network Topology
Configuration
Novell eDirectory Configuration
WLC Configuration
Client Configuration
Debugs
Related Information

Introduction

In the K−12 education space, there has been an increasing need to authenticate wireless users via accounts created within Novell's eDirectory. Due to the distributed nature of the K−12 environment, the individual schools might not have the resources to place a RADIUS server at every site nor do they desire the additional overhead of configuring these RADIUS servers. The only way to accomplish this is by using LDAP to communicate between the Wireless LAN Controller (WLC) and an LDAP server. Cisco Wireless LAN Controllers support Local EAP authentication against external LDAP databases such as Microsoft Active Directory. This white paper documents a Cisco WLC configured for Local EAP Authentication against Novell's eDirectory enabled as a full−featured LDAP server. One caveat to note the tested clients were using Cisco Aironet Desktop Utility to perform 802.1x authentication. Novell currently does not support 802.1x with their client at this time. As a result, depending on the client, a two−stage login process could occur. Note these references:

Novell 802.1x Statement

"Currently, they must log in twice. When the Novell Client is installed, a user must log in using the Workstation Only check box on the initial login dialog to allow 802.1x user authentication when the desktop is initialized, and then they must log in to the Novell network using the "red N" login utility. This is referred to as a two−stage login."

An alternative to the "workstation only login" is to configure the Novell Client to use "Initial Novell Login=Off" in the Advanced Login settings (the default is "Initial Novell Login=On"). For more information, refer to 802.1x Authentication and the Novell Client for Windows .

Third party clients such as Meetinghouse Aeigs Client (Cisco Secure Services Client) a Novell Technology Partner may not require a double login. For more information, refer to AEGIS SecureConnect .

Another viable workaround for the Novell client is to have the machine (or user) authenticate (802.1x) to the WLAN prior to the Novell GINA being executed.

Testing a solution for Single Sign On with the Novell client and 802.1x is beyond the scope of this white

paper.

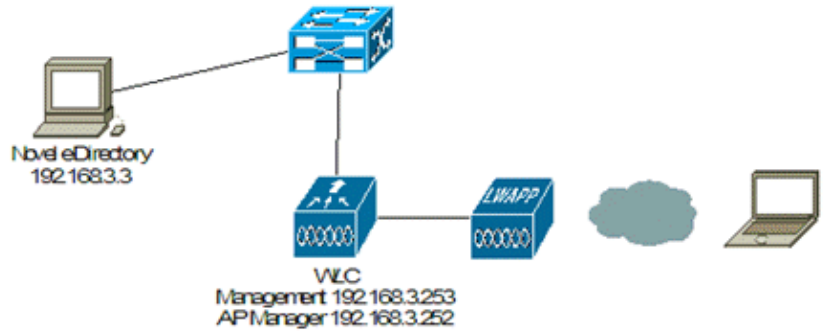
Tested Topology

Solution Tested

- Cisco Wireless LAN Controller with 6.0.188.0 software
- Cisco Aironet LWAPP AP 1242AG
- Windows XP with Cisco Aironet Desktop Utility 4.4
- Windows Server 2003 with Novell eDirectory 8.8,5
- Novell ConsoleOne 1.3.6h (eDirectory management utility)

Network Topology

Figure 1



Device	IP Address	Subnet Mask	Default Gateway
Novell eDirectory	192.168.3.3	255.255.255.0	192.168.3.254
Layer 3 Switch	192.168.3.254	255.255.255.0	–
AP	Assigned via DHCP from L3 Switch	255.255.255.0	192.168.3.254
WLC Management Interface WLC AP Manager Interface	192.168.3.253 192.168.3.252	255.255.255.0	192.168.3.254

Configuration

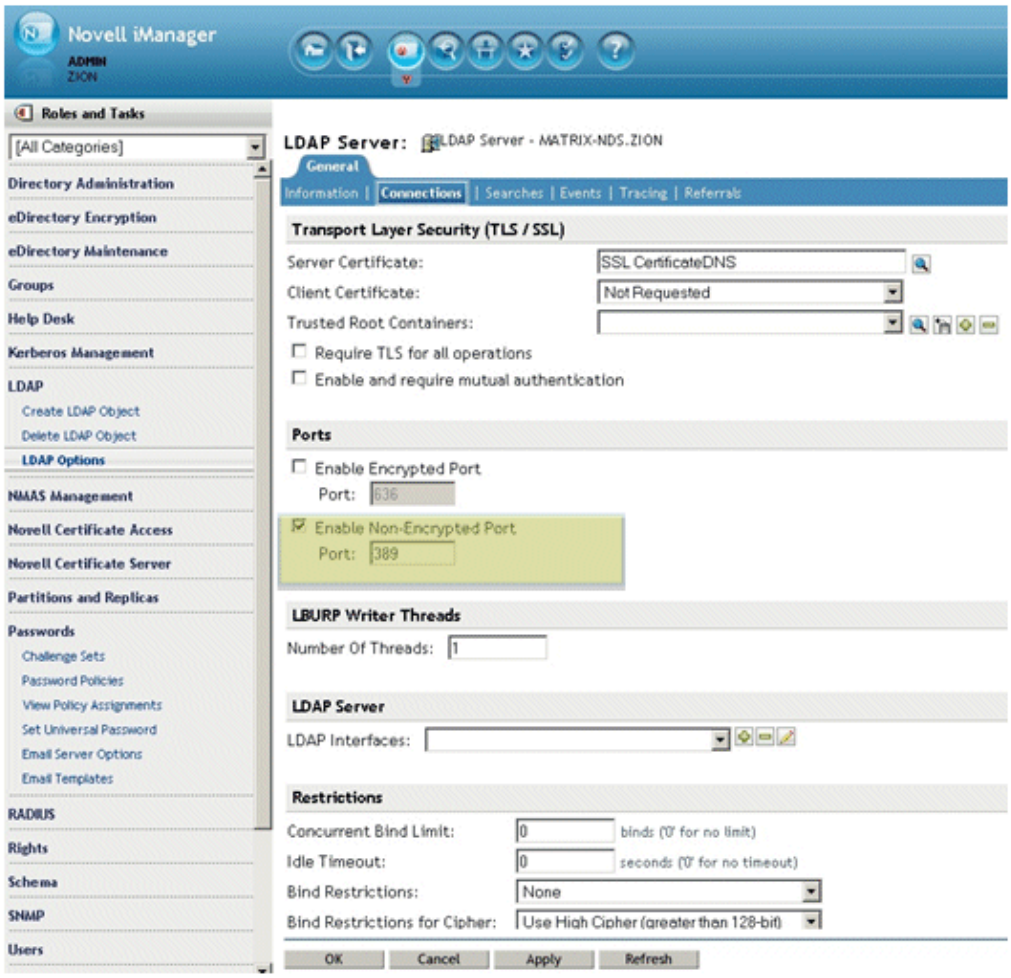
Novell eDirectory Configuration

Full Novell eDirectory installation and configuration is beyond the scope of this white paper. Novell eDirectory must be installed as well as the corresponding LDAP components.

Key configuration parameters required are that Simple Password must be enabled for the user accounts and Authenticated LDAP must be configured. Using TLS for LDAP was supported in previous versions of WLC code (4.2); however, Secure LDAP is no longer supported on the Cisco WLAN Controller software.

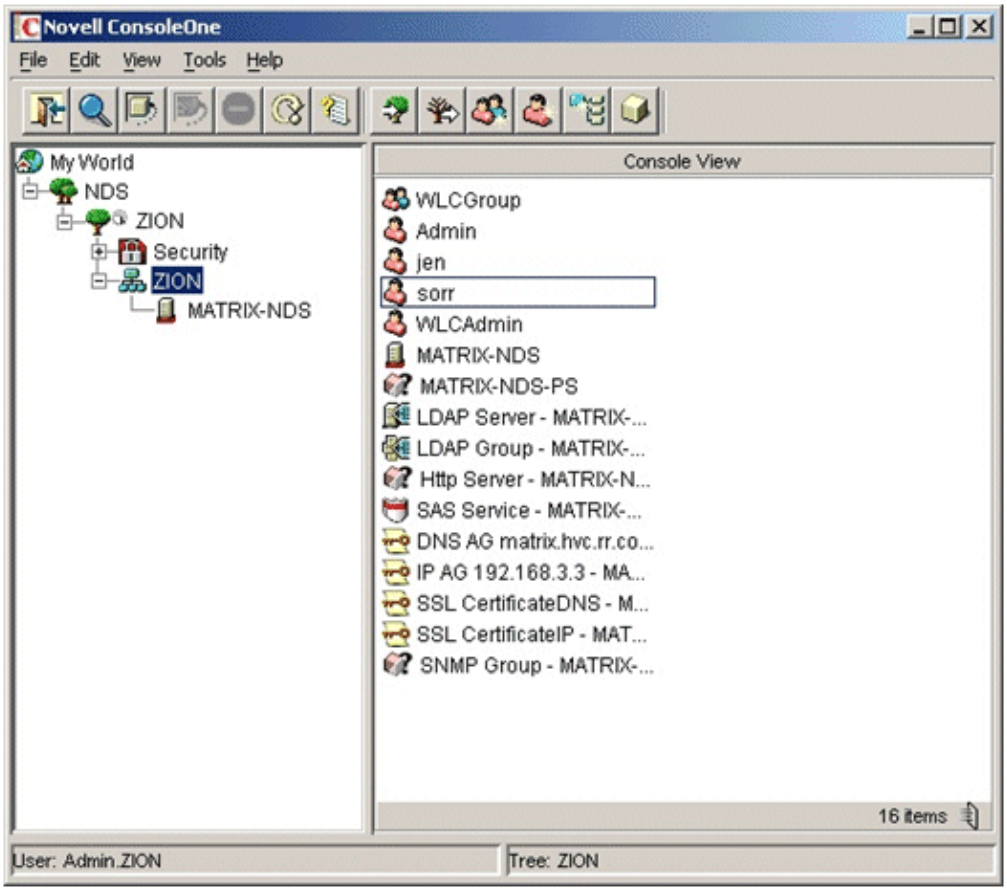
1. When configuring the LDAP server portion of eDirectory, make sure that the Non−Encrypted LDAP ports (389) are enabled. See Figure 2 from the Novell iManager application.

   Figure 2



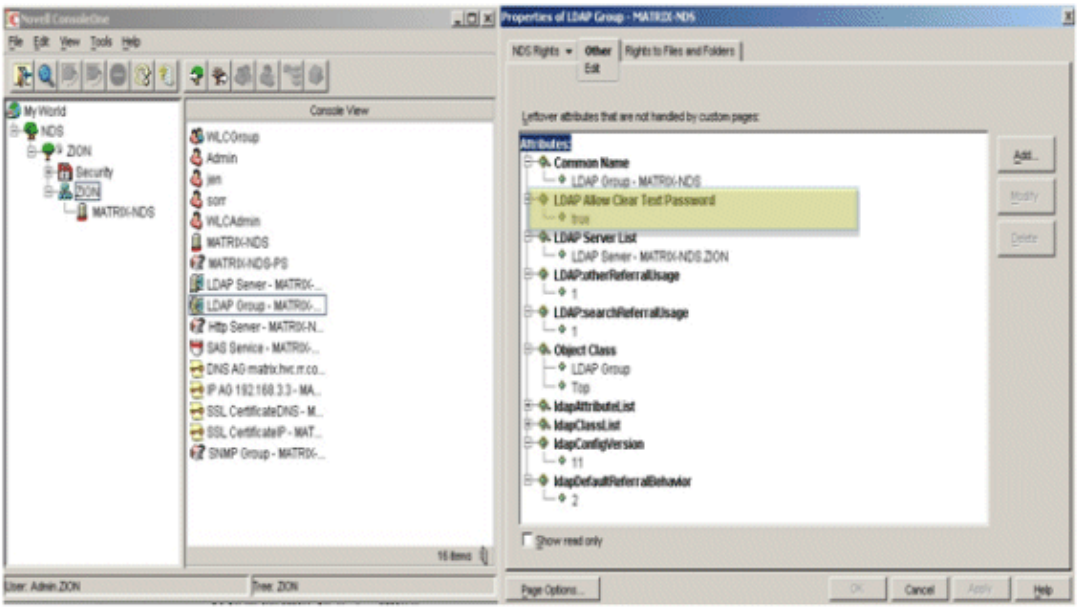
2. During the eDirectory installation, it will ask you for the Tree structure or Domain Name, etc. If eDirectory is already installed, Novell's ConsoleOne (Figure 3) is an easy tool by which to view the eDirectory structure. It is critical to find what the appropriate schemas are when trying to establish communication to the WLC. You must also have an account created that will allow the WLC to perform an Authenticated Bind to the LDAP server. For simplicity, in this case, the Novell eDirecotry Admin account is used for the Authenticated Bind.

   Figure 3



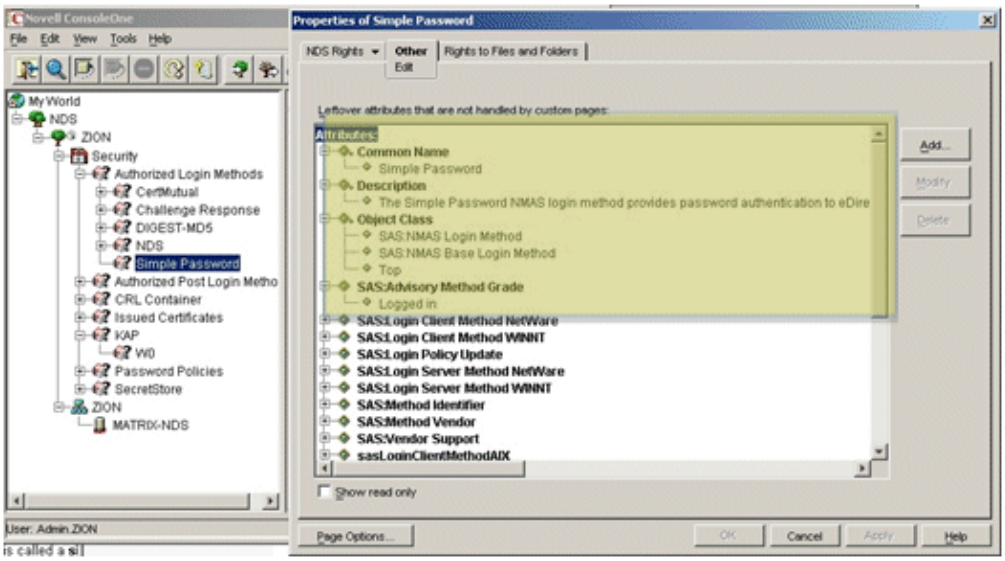
3. Use ConsoleOne in order to verify that the LDAP group allows **Clear Text Passwords**.

Figure 4



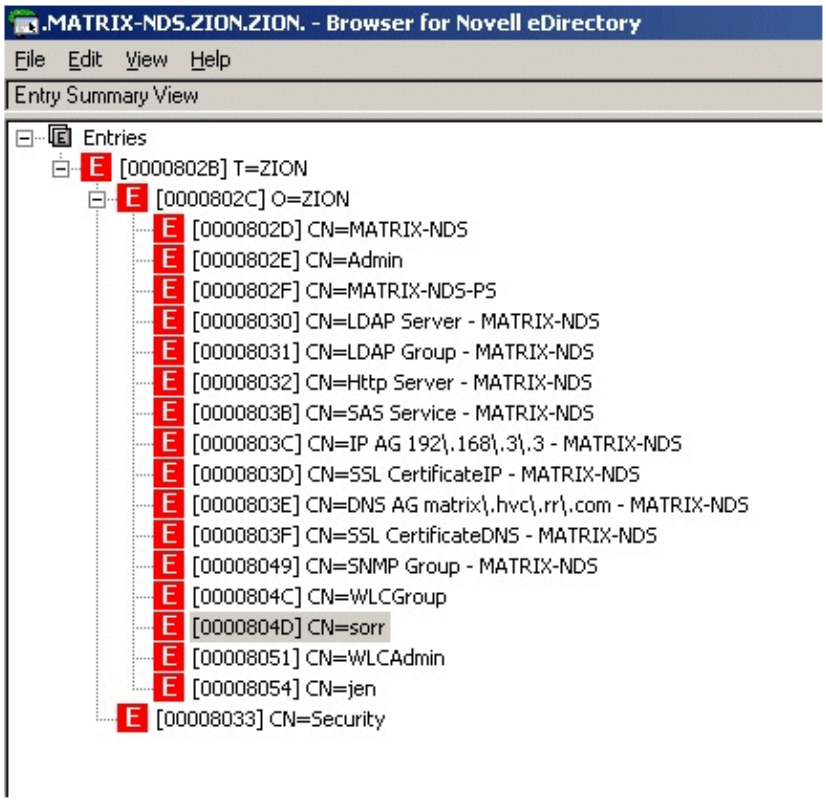
4. Verify that under the OU, Security settings that **Simple Password** is enabled.

Figure 5



Another useful tool by which to view the Novell eDirectory structure is the browser included with the default installation.

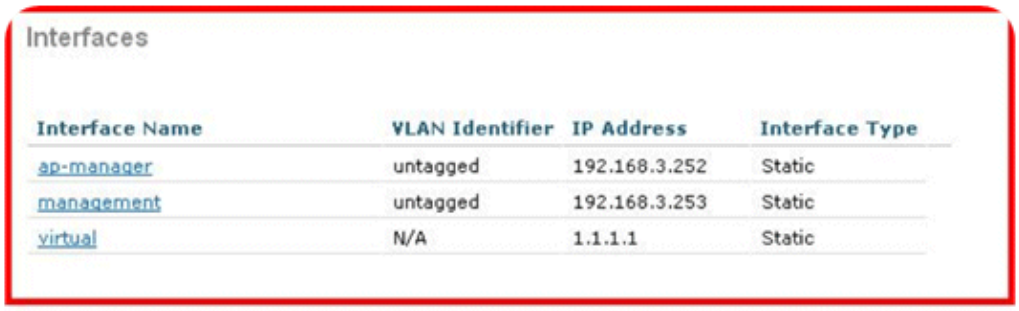
Figure 6



WLC Configuration

Refer to Figure 1 for the physical topology of the test network. The WLC used in this test was configured according to standard practice with both AP−Manager and Management interfaces on the same subnet and untagged from a VLAN perspective.

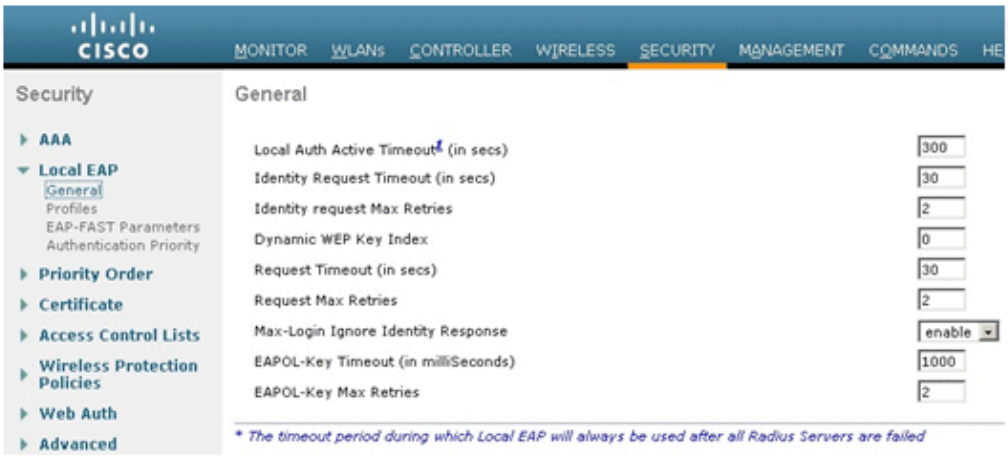
Figure 7



1. Configure Local EAP Authentication: **Security** > **Local EAP** > **General**.

   Standard defaults were not changed.

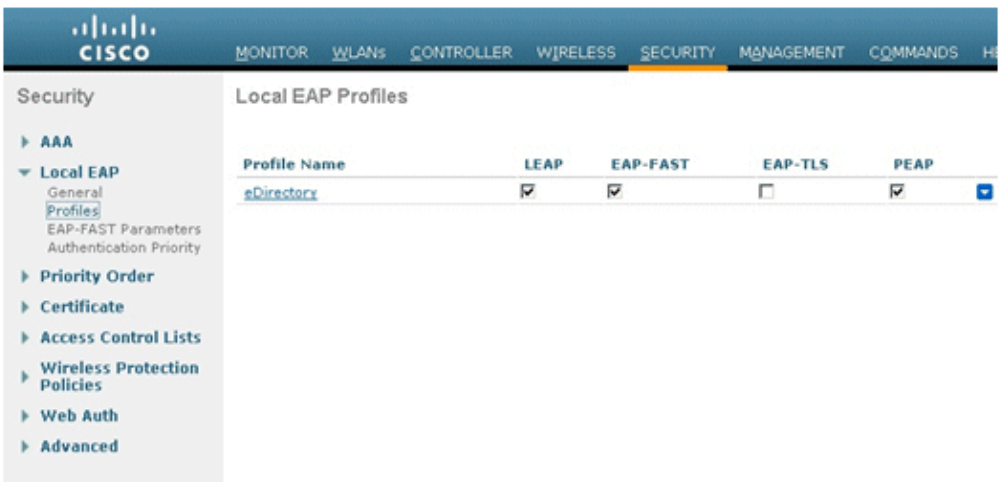
   Figure 8



2. Create a new Local EAP Profile: **Security** > **Local EAP** > **Profiles**.

   For this test case, the Local EAP profile name chosen was eDirectory. Authentication methods chosen were LEAP, EAP−FAST and PEAP; however, only PEAP was tested in this document.

   Figure 9



   When you configure Local EAP Authentication for PEAP, you must have a certificate installed on the WLC. In this case, for testing purposes, the factory installed Cisco certificate was used; however, a customer provisioned certificate can also be installed. Client−side certificates are not required for the

use of PEAP−GTC, but they can be enabled for the Inner PEAP method if required.

Figure 10

3. Set the Authentication Priority for LDAP: **Security** > **Local EAP** > **Authentication Priority**.

Figure 11

4. Add the LDAP server to the WLC: **Security** > **AAA** > **LDAP**.

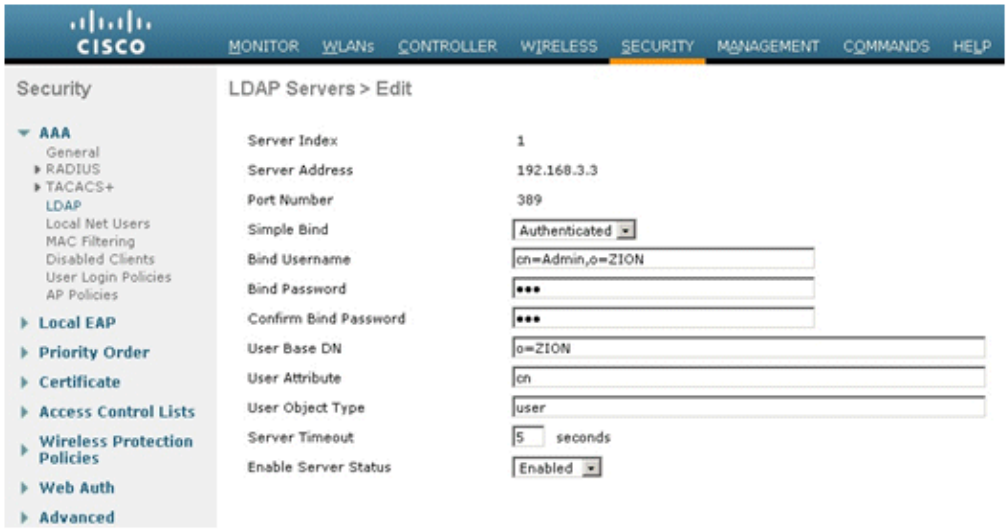
Figure 12

5. Configure the WLC to use Novel eDirecotry (see Figure 13):

    a. Choose **Authenticated** for the Simple Bind method.
    b. Enter the Bind Username. This is the account that was created to within eDirectory that will be used for the WLC to bind to eDirectory.

    Note: Make sure that you enter the correct directory attributes for the username. For this test case, "cn=Admin,o=ZION" was used.
    c. Enter the Bind Password. This is the password for the Bind user account.
    d. Enter the User Base DN. This is the Domain Name where the wireless user accounts are located. In the test case, the users were located at the root of the DN (o=Zion). If they are nested within other groups/organizations, chain them together with a comma (for example, "o=ZION,o=WLCUser").
    e. Enter the User Attribute. This is the Common Name (CN) (see Figure 6).
    f. User Object Type This is set to *user*.

Figure 13



6. Create the WLAN that you want the Novell eDirectory clients to use. For this test case, the WLAN Profile name is *eDirectory* and the SSID is *Novell* (see Figure 14).

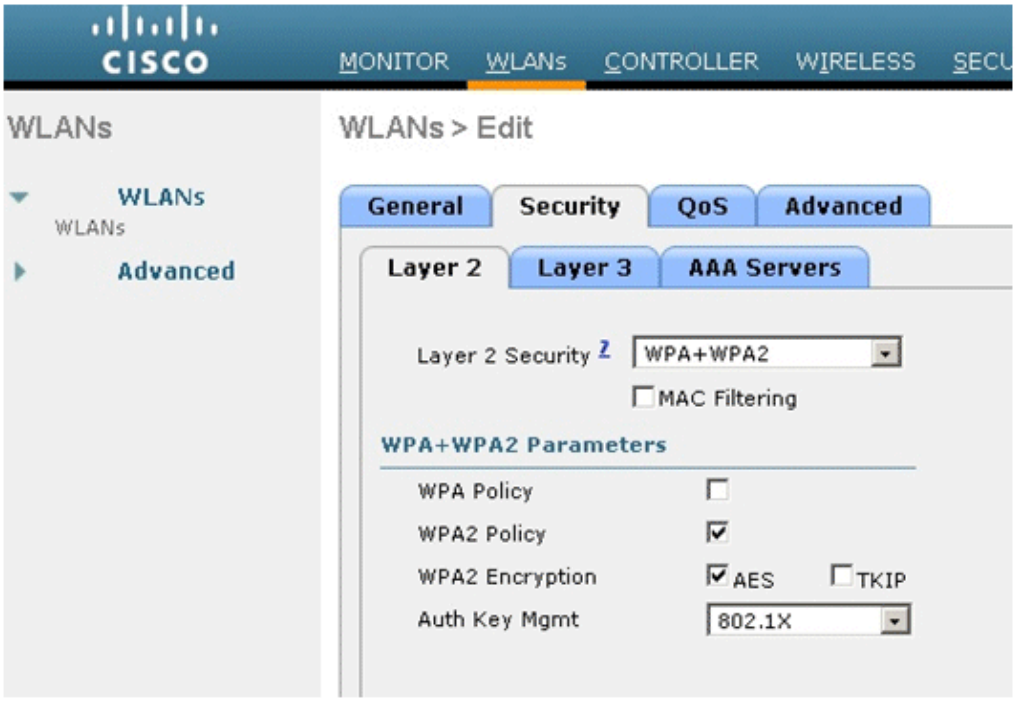
Figure 14

7. Enable the WLAN and apply the appropriate radio policy and interface. For this test case, the Novell SSID was only enabled for the 802.11a network and was tied to the management interface.

Figure 15

8. Configure the appropriate Layer 2 Security settings. For this test case, WPA+WPA2 Security, WPA2 policy, AES encryption, and 802.1x for Key Management were selected.

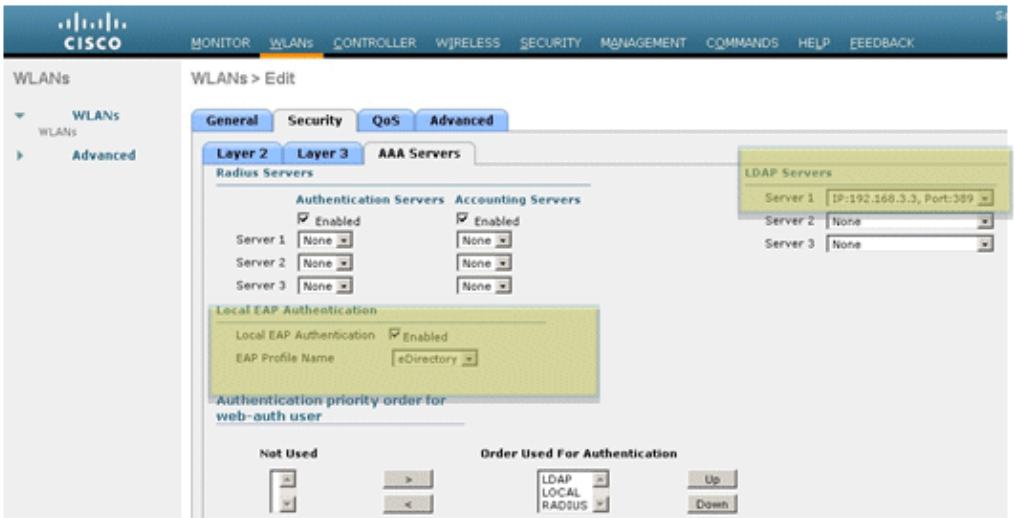
Figure 16



9. To complete the Local EAP Authentication configuration, configure the WLAN for Local EAP authentication using the LDAP server:

    a. Choose **Local EAP Authentication Enabled** and apply the created EAP Profile (**eDirectory**).
    b. Under the LDAP servers, choose the IP Address of the configured eDirectory server (**192.168.3.3**).

Figure 17



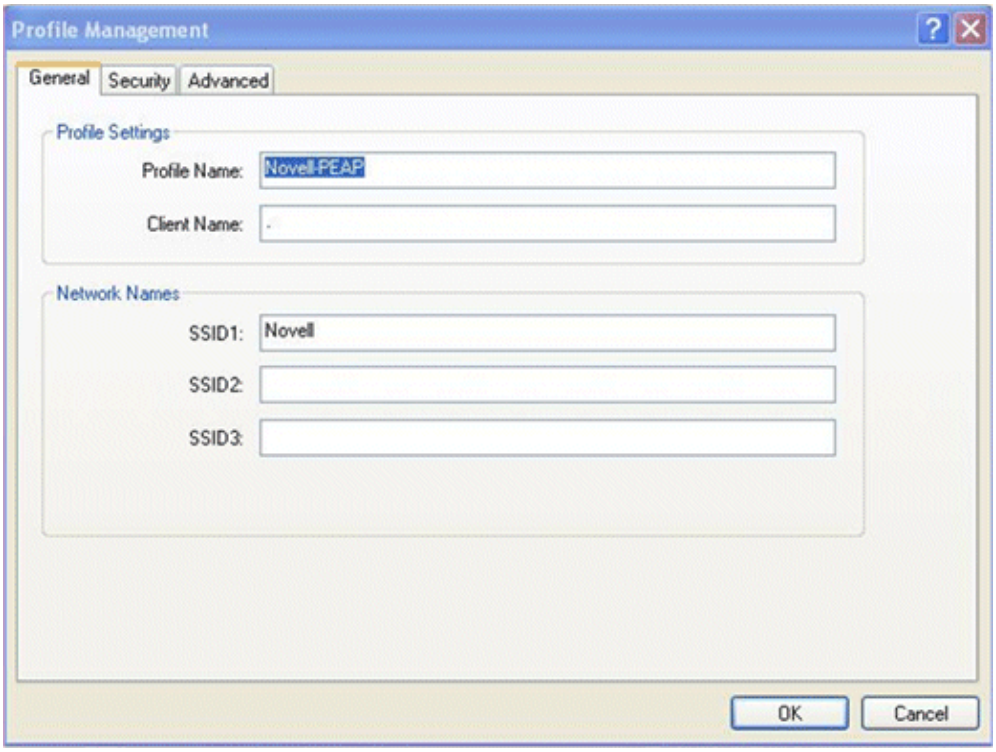
Client Configuration

PEAP−GTC is the current authentication requirement for the majority of the K−12 schools. WLC does not support MSCHAPv2 for Local EAP Authentication. As a result, you must choose GTC for the EAP Authentication type on the client.

The following figures are a walkthrough of the Cisco Aironet Desktop Utility configuration for PEAP−GTC to connect to the WLAN SSID Novell. Similar configurations are achieved with the native Microsoft client with PEAP−GTC support.

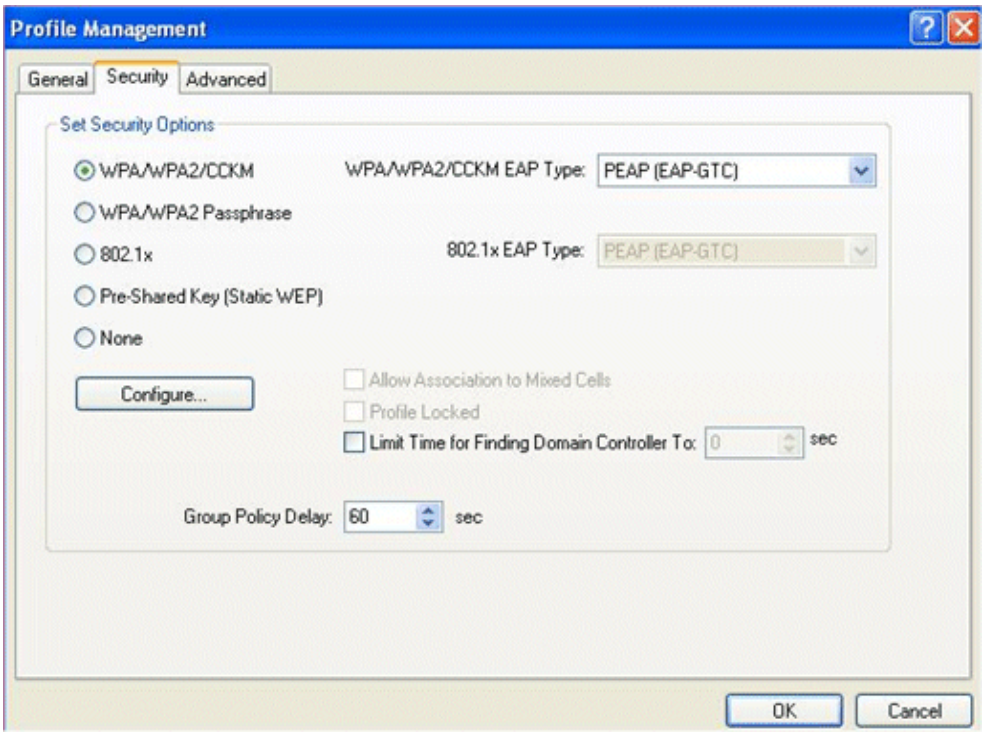
1. Configure the Client Profile Name and SSID (Novell).

Figure 18



2. Choose **WPA/WPA2/CCKM** for Security and **PEAP (EAP−GTC)** for the EAP type.

Figure 19



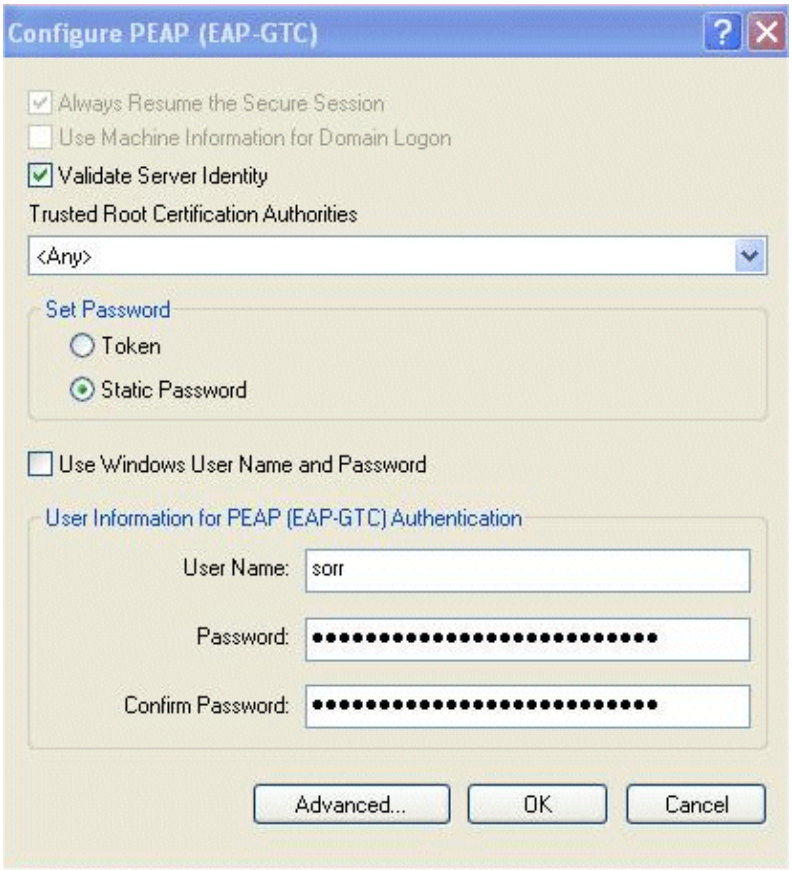
3. Configure PEAP−GTC:

   a. Choose **Validate Server Identity** and **Static Password**.
   b. Enter the username and password for the account or the supplicant will prompt for the

credentials at logon.

c. Do not enter in the **<ANY>** Novell directory schema, as this is not required.

Figure 20



4. Once the profile is completed, activate it and the authentication process should begin.

Figure 21

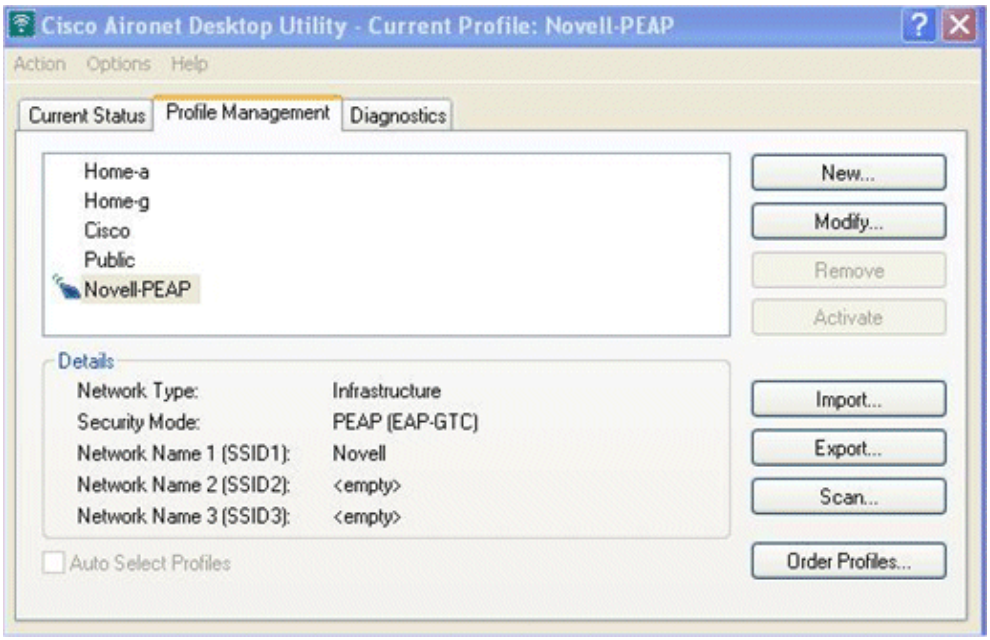
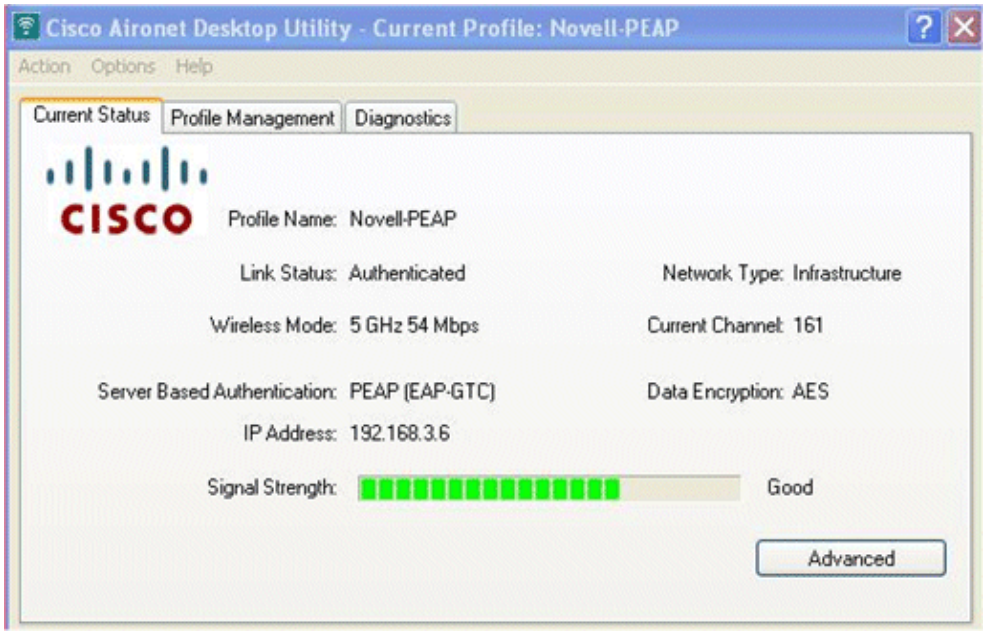


Figure 22 depicts a successful Association and Authentication via PEAP−GTC.

Figure 22

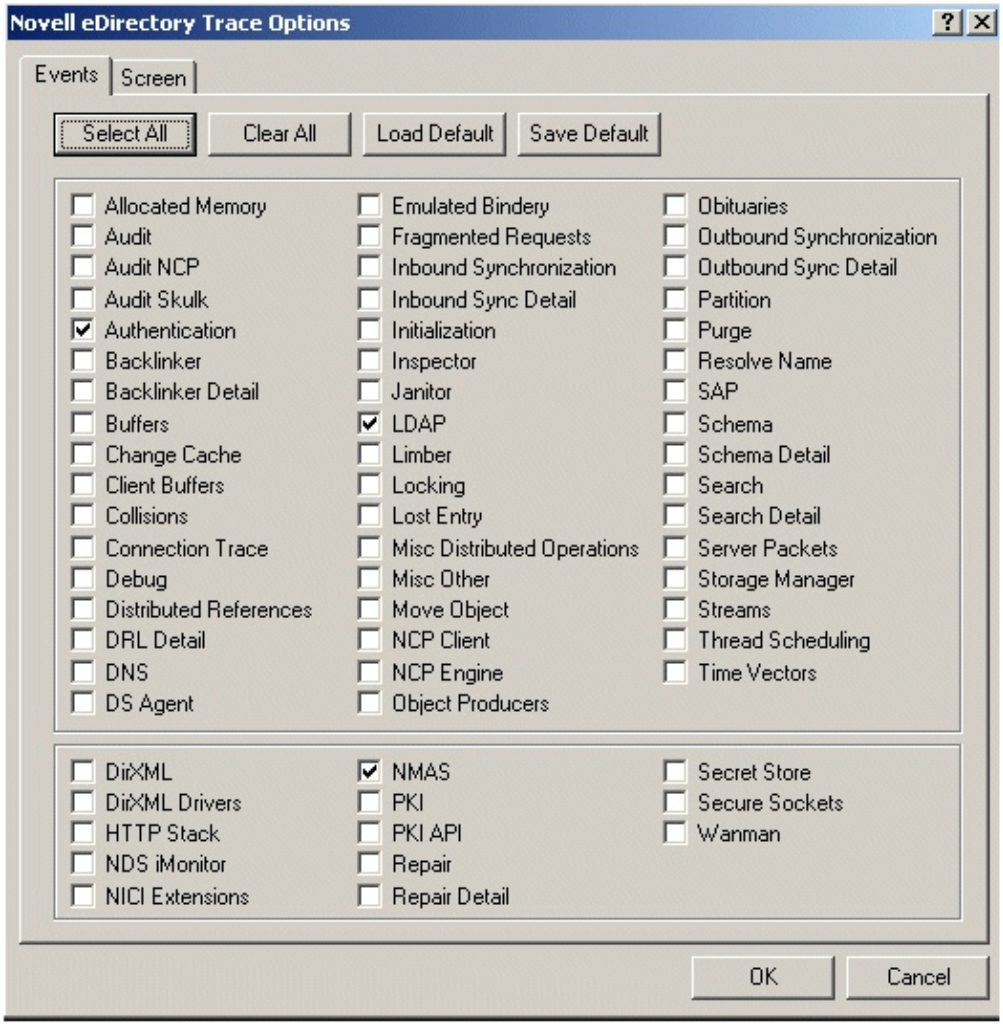


Debugs

To verify that you are able to perform an authenticated BIND as well as user authentication, enable these trace options for eDirectory:

- **Authentication**
- **LDAP**
- **NMAS**

Figure 23



As shown in the debug, a successful LDAP authentication response is delivered to the Wireless LAN controller at 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
```

Note: Some of the lines in the debug output have been wrapped due to space constraints.

To ensure that the WLC is making a successful Authentication request to the eDirectory server, issue these **debug** commands on the WLC:

```
debug aaa ldap enable

debug aaa local-auth eap method events enable

debug aaa local-auth db enable
```

Sample output from a successful authentication:

```
*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
```

Note: Some of the lines in the output have been wrapped due to space constraints.

As more K−12 schools adopt the Cisco WLAN architecture, there will be an increasing need to support wireless user authentication to Novell's eDirectory. This paper has verified that a Cisco WLC can authenticate users against Novell's eDirectory LDAP database when configured for Local EAP Authentication. A similar configuration can also be done with Cisco Secure ACS authenticating users to Novell's eDirectory. Further investigation must be done for Single Sign On with other WLAN clients such as Cisco Secure Services Client and Microsoft Windows Zero configuration.

Related Information

- **Local EAP Authentication on the Wireless LAN Controller with EAP−FAST and LDAP Server Configuration Example**
- **Unified Wireless Network Local EAP Server Configuration Example**
- **EAP−FAST Authentication with Wireless LAN Controllers and External RADIUS Server Configuration Example**
- **Technical Support & Documentation − Cisco Systems**

Updated: Oct 07, 2010 Document ID: 112137