

# Securing Wireless LANs with LDAP



Many organizations have standardized on LDAP (Lightweight Directory Access Protocol) servers as a repository for their users and related security information. Some examples of these include: Apple Open Directory, OpenLDAP, Microsoft Active Directory and others.

The challenge for these organizations comes when they attempt to add 802.11 wireless access to their existing network. Current Wi-Fi best practice is to encrypt all over-the-air transmissions between the wireless client and the network as well as authenticate each device and user. The obvious solution for many organizations is to adopt a strong encryption protocol (802.11i (WPA2) with AES is highly recommended) and authenticate users against the existing directory server since that is where this information exists.

But the obvious solution does not offer full support for LDAP-based organizations. Specifically, WPA2 include the IEEE 802.1X protocol and EAP (Extensible Authentication Protocols). These protocols handle communications between a wireless client, the authenticator (AP or WLAN controller) and a backend authentication server. Currently, 802.1X and the various EAP methods have limited support for an LDAP authentication server.

## New Dynamic Pre-shared Key (PSK) technology offers strong encryption, native LDAP authentication and network access without any third-party client software

### Why 802.1X and PEAP Don't Work with LDAP

The issue is the user password and how it is handled. The most popular Wi-Fi clients use WPA/WPA2 and EAP-PEAP as the method for authentication, network access and encryption. But this client combination has several problems with LDAP. Specifically:

- The 802.1X standard, which is part of WPA and WPA2, does not support native communications with LDAP, only RADIUS.

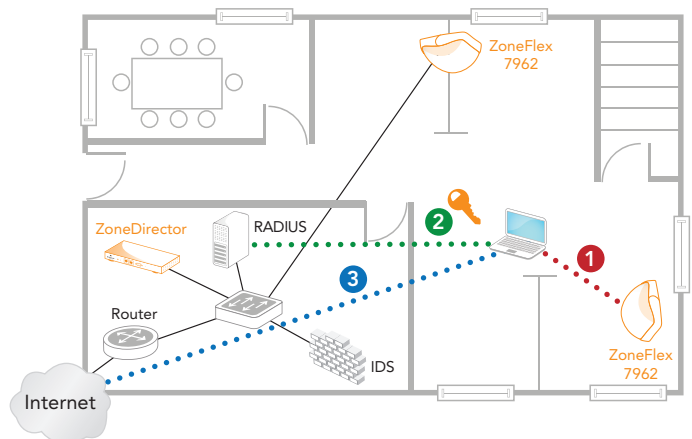
- The PEAP mechanism, the most popular and widely supported authentication for WPA and WPA2, only supports passwords that are stored in an NT (Windows) format.

### 802.1X Difficulties for LDAP

The IEEE 802.1X standard (the latest version is officially called 802.1X-2004) provides port-based authentication for the wireless network. This involves communications between a supplicant (wireless client device), authenticator (access point or WLAN controller), and authentication server. Upon detection of a new client (supplicant), the authenticator sets the client to an unauthorized state. In this state, only 802.1X traffic is allowed; other traffic, such as DHCP or HTTP, is blocked. The authenticator sends an EAP-Request identity to the supplicant, the supplicant responds with the EAP-response packet that the authenticator forwards to the authenticating server. If the authentication server accepts the request, the authenticator sets the client as authorized and normal traffic is allowed (See Figure 1).

The 802.1X standard was written to communicate with IETF AAA (Authentication, Access Control and Accounting) compliant

**FIGURE 1:** Using 802.1X, a wireless node must be authenticated to a RADIUS server before it can gain access to the wireless LAN



1. User associates to wireless LAN.
2. AP requests identity of user and sends responses to authentication RADIUS server.
3. Client is authorized and data traffic is allowed to Internet.

servers. Currently, these include: RADIUS, DIAMETER, TACACS and TACACS+. All of these servers communicate using the RADIUS (Remote Authentication Dial In User Service) protocol. There is no definition for LDAP in this standard, which means direct communications between a supplicant/authenticator and a directory server is not supported.

One way to get around this limitation is to install a RADIUS server as a front-end for a directory server. The authenticator communicates with RADIUS, which then communicates natively with the back-end server. This is a very common scenario, particularly when the directory server is Microsoft's Active Directory. However, even using a RADIUS server in front of an LDAP server is not always possible. The reason for this is the second half of the problem, PEAP (Protected Extensible Authentication Protocol).

### Compatibility Issues Between PEAP and LDAP

802.1X requires an EAP mechanism of some kind for the actual authentication process. The most popular EAP that client supplicants support is EAP-PEAP, commonly referred to as simply PEAP. Unlike other EAP methods, PEAP is not an encryption protocol. It only authenticates the client to an authentication server. PEAP uses server-side certificates to authenticate the server so that it doesn't mistakenly send user credentials to an imposter. Once the server has been validated, an encrypted SSL/TLS tunnel is setup between the client and the authentication server. Once the encrypted tunnel is established, a second protocol (MS-CHAPv2) is used to securely transmit the user credentials to the authentication server.

MS-CHAPv2, which is the only protocol handling user credentials, sends the user name and a one-way hash of the user password. This hash is compared to the hash stored on the authentication server. This is where the problem lies for LDAP authentication servers. The MS-CHAPv2 protocol can only use one type of hash on the password, an NT hash. With the exception of Active Directory, few other directory servers store user passwords as an NT hash. Typically, they use SHA-1 or MD5, both of which are incompatible with the NT hash format. Since hashes are one-way and not reversible, there is no way to reverse engineer or decrypt them into another format without having the original clear text password.

Since Active Directory stores user passwords as NT hashes, it is compatible with PEAP. But options are limited for non-Microsoft LDAP servers or organizations that do not wish to deploy a RADIUS server in front of Active Directory. One work

around is to use an EAP that does not use NT hashes or Microsoft-based authentication. The only real alternative is **EAP-GTC**. This is supported by PEAP as an alternative inner protocol to MS-CHAPv2. However there is no native OS support for it, so it requires a third-party client be installed.

Technically, EAP-GTC is a valid alternative to PEAP-MS-CHAPv2. Realistically, support for EAP-GTC would involve just as much hassle with the cost to acquire a client and install, configure and support it on every wireless device.

### Dynamic PSK: A Simple and Secure Alternative

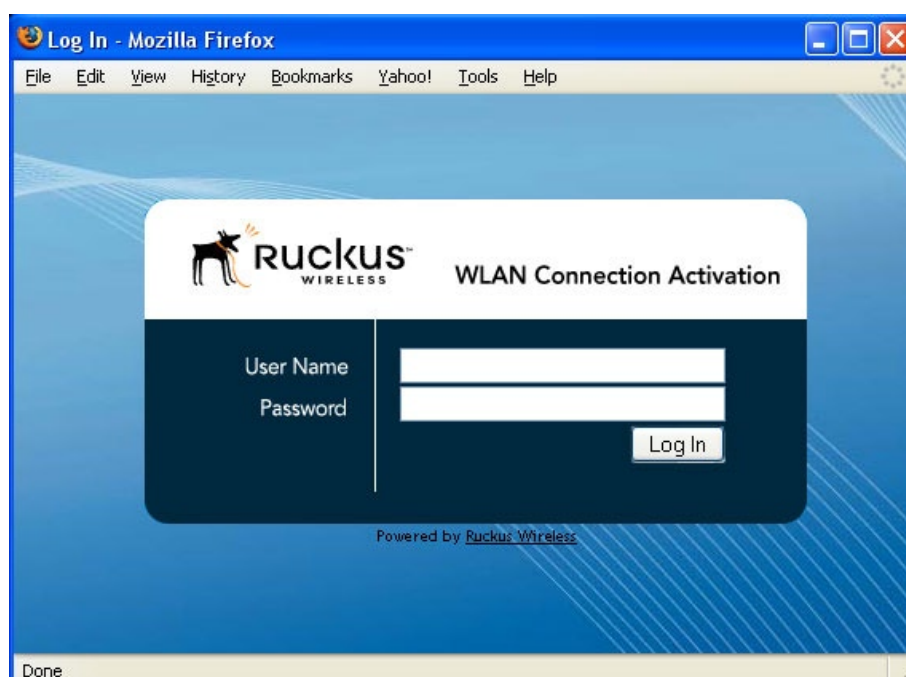
A very reasonable alternative exists that offers strong encryption, native LDAP authentication and network access without requiring third-party software: *Dynamic Pre-shared Keys (PSK)*.

#### How Dynamic PSK Works

With Ruckus Dynamic PSK, the following process occurs:

1. A user's device is activated
  - Activation grants a wireless device a unique key (Dynamic Pre-Shared Key) that identifies it to the wireless LAN and ensures encryption takes place for all traffic (including user credentials).
2. The device is connected to the wireless LAN
3. The user enters their own credentials into a web login page
4. The credentials are authenticated directly with the directory server
5. If successful, the user is granted access

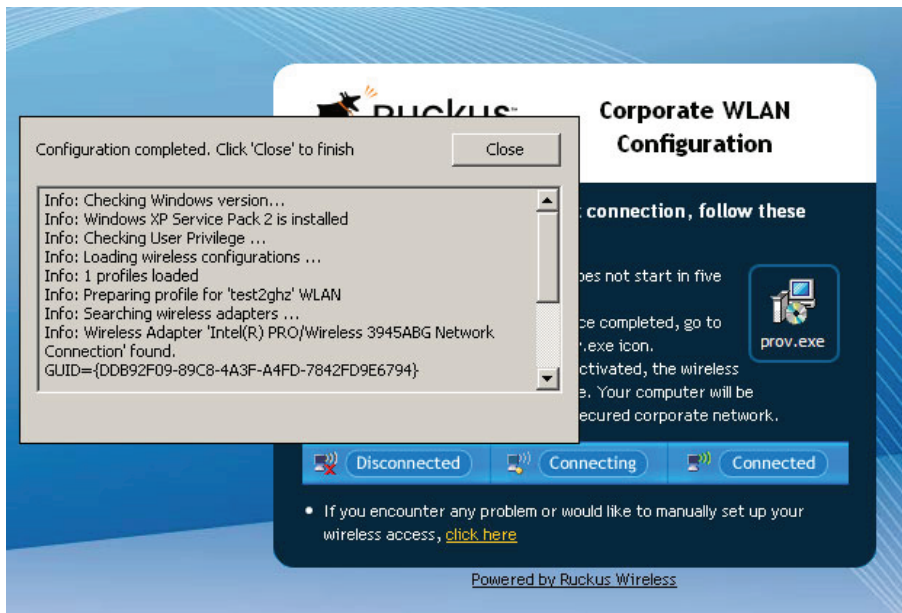
Figure 2: Activating the client



The first step, device activation, can be self-service for users or an administrative function. In either case, the user connects the device to the network (wired or wireless) and points their browser at the ZoneDirector activation web page (<https://<zonedirector>/activate>). The user is prompted to enter his or her own credentials, which are checked against the directory server and receives a unique key to access the wireless network (See Figure 2).

If successful, the user is directed to a new Web page that automatically configures the client system (See Figure 3).

**Figure 3:** Configuring the client (Windows automation)



If the device is a Windows machine, an iPhone or Windows CE system, a script will automatically configure the client to connect to the WLANs that the administrator has designated to be used with the Dynamic Pre-Shared Key (See Figure 4).

This displays a window with everything needed to configure the device to connect with the WLAN: the SSID, authentication and encryption type as well as their unique personal access key (See Figure 5).

They can simply cut and paste the information. This unique key is stored in a central database (the ZoneDirector internal database). Each key will only work for the device it was issued to and can include an expiration date after which the key will no longer work. Keys are easily managed or revoked on an individual basis. This is quite different from a normal PSK network in which each device shares the same encryption key.

So far, Dynamic PSK has ensured secure and private communications for the wireless device on the WLAN. However this does not ensure that the user is a valid identity stored in the directory server. To accomplish this, a Captive Portal login

page is configured. This will present the user with a login page (See Figure 6). The credentials entered are then checked against the directory server and the connection is authorized if the check is successful. And unsuccessful authentication attempt will leave the user and device with no network access.

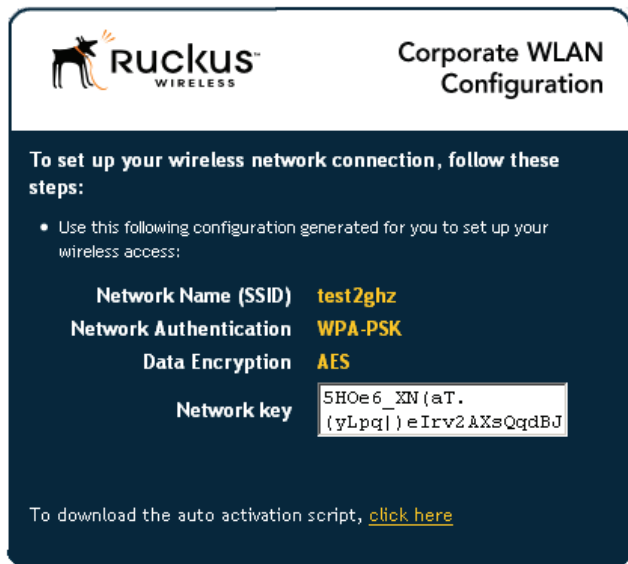
Dynamic Pre-shared Keys (PSK) eliminates the hassle and incompatibility issues between directory servers while maintaining wireless security and authentication. The key is to eliminate the source of the incompatibilities, 802.1X and PEAP, while still maintaining strong, user-based encryption, and identity checks and authorization.

The self-service feature of Dynamic PSK gives IT organizations the option to allow authorized users to set up their own machines themselves in a safe, secure manner that does not compromise the security of any other wireless device or user. Network access is always associated with a valid user identity. Configuration is as simple as cutting and pasting a key and entering their user name and passwords on a web page. Wireless device support is universal since any modern wireless device supports pre-shared keys and web browsers.

The simplicity of Dynamic PSK can dramatically reduce the cost and speed of implementing a secure WLAN without sacrificing encryption or user authentication.

**Figure 4:** Configuring the client (manually)



**Figure 5:** Displaying the WLAN network key (manually)

## CONFIGURING THE ZONEDIRECTOR

All management of authentication servers is performed by the ZoneDirector. Simple-to-use menus guide IT administrators through the process of enabling LDAP authentication such as Apple's Directory Service. To enable Dynamic PSK and Captive Portal, administrators simply click a check box within the setup wizard. From there, managers can see associated clients and keys and make any desired changes.

In this example we are using an Active Directory server. This could be any LDAP server such as Apple's Directory Server or even RADIUS (See Figure 7).

## Configure the WLAN

In the WLAN (named ruckus), we have enabled both Dynamic PSK and Zero-IT Activation. Zero-IT allows Windows users to download a script at activation time, which will automatically configure their wireless card for all wireless networks to which they now have access. This makes wireless even easier to deploy since users can essentially self-provision themselves while still being forced to produce valid authenticated credentials first (See Figure 8).

## Manage Keys

At any time, an administrator has the option of examining keys that are currently in use and the users to whom each key belongs.

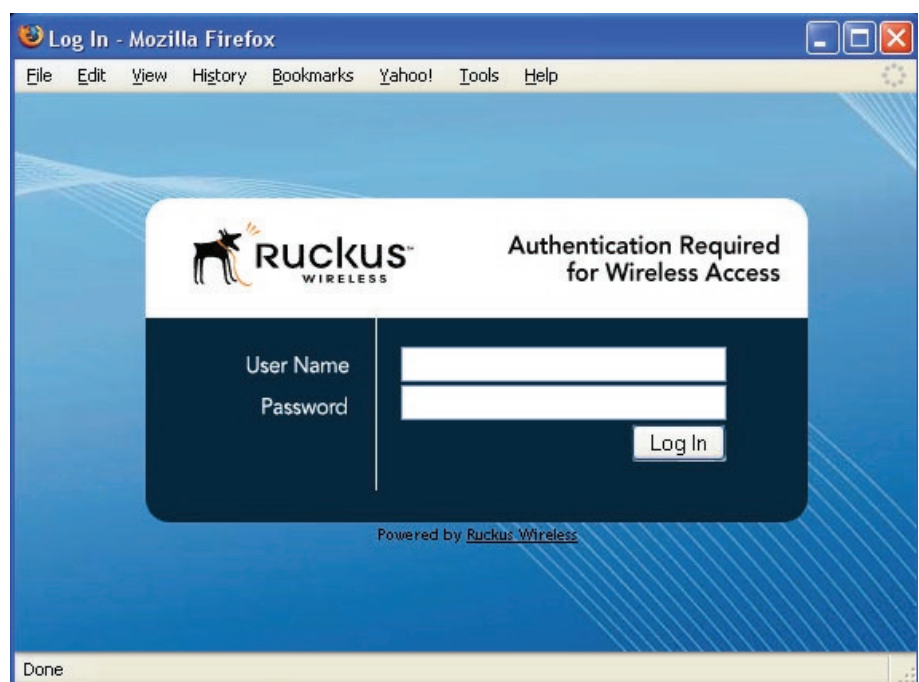
Administrators can delete keys at any time. They can also change the authentication server or the amount of time a Dynamic PSK may be used before they automatically expire (See Figure 9).

## Summary

Schools and other organizations that have standardized on directory servers (LDAP) and wish to deploy wireless LANs are unfairly penalized by current wireless security standards. These standards require either an additional RADIUS server that must be installed, configured and maintained or poorly supported protocols that require third-party clients. The result is an infrastructure that adds complexity without delivering equal value for the hassle and cost.

Dynamic PSK from Ruckus Wireless offer a unique way to secure wireless LANs for organizations that use LDAP as their backend authentication server of choice. Dynamic PSK is robust, secure, and easily managed. It does not require additional servers, protocols or client software. Instead it leverages well-developed and supported clients that are native to most operating systems and easily supported by IT.

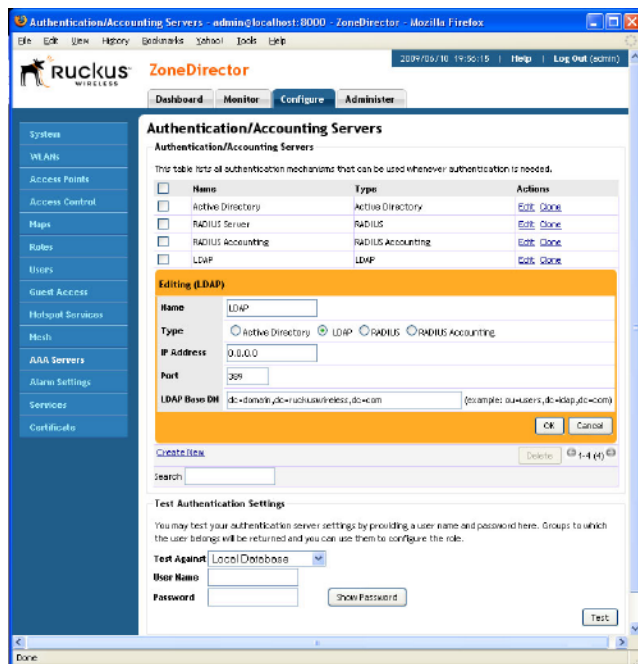
- **No 802.1X dependency** — without 802.1X, there is no need for a wireless-enabled RADIUS server. Authentication can occur natively against LDAP. No extra servers and protocols to manage.
- **Standards-based WPA2 security** — all of the other great features of WPA and WPA2 (such as ultra-strong AES encryption) are available to secure over-the-air communications.

**Figure 6:** Displaying the WLAN network key (manually)

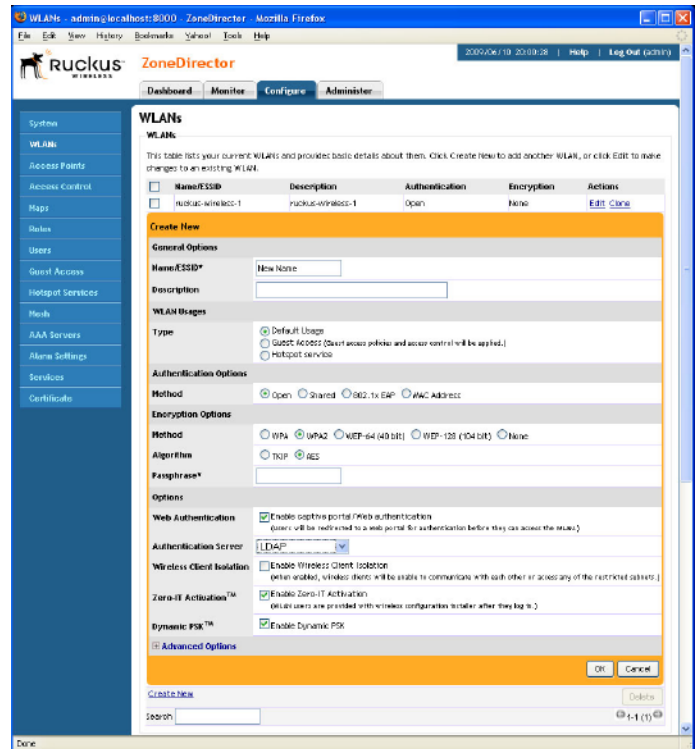
- **Native OS support** — most popular operating systems support this today with no modification or third-party software necessary.
- **Easy to implement** — traditionally, networks based on pre-shared keys (PSK) require manual administrator intervention to configure client devices with the PSK.
- **Secure** — unlike typical PSK networks, which share a single key amongst all devices, a Dynamic PSK network assigns a unique key to every authenticated user. Therefore, when a persona leaves the organization, network administrators do not need to change the key on every device. Only that person's unique key must be deleted, which can quickly be done from a central management console.

Dynamic PSK networks are the sensible and most reasonable way to deploy wireless LANs in conjunction with LDAP authentication. They offer the latest in security, authentication and encryption without sacrificing ease of use or IT cycles in support of additional unwanted equipment or help desk calls.

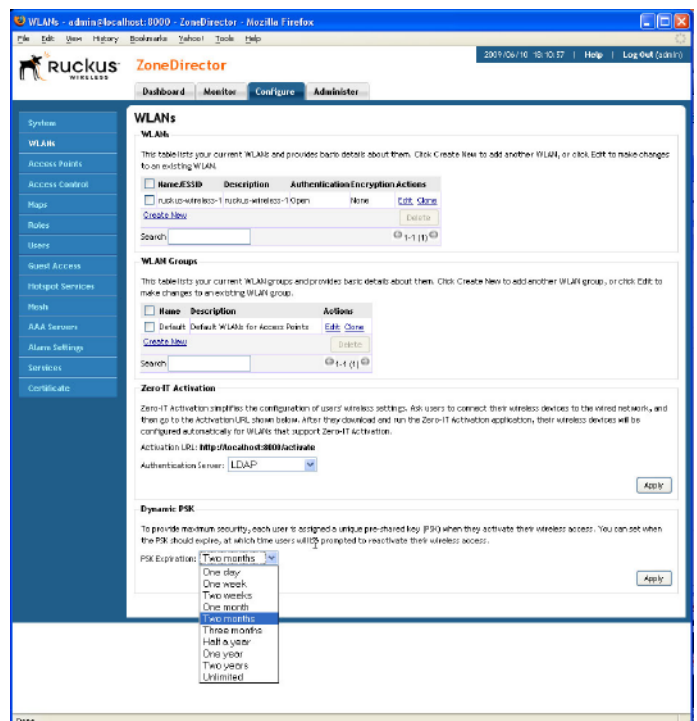
**Figure 7:** Authentication servers screen allows the choice of LDAP, AD or RADIUS servers.



**Figure 8:** Setup SSIDs on this screen and enabled the Dynamic PSK (through the Zero IT Activation radio button) for automatic configuration of client devices.



**Figure 9:** Administrators can view, search and delete Dynamic Pre Shared Keys from this screen. Choose authentication server options and Dynamic PSK expiration times.



## Appendix

### Excellent Reading

*Port-Based Authentication with 802.1X*

[http://www.wireless-nets.com/resources/downloads/802.1X\\_C2.html](http://www.wireless-nets.com/resources/downloads/802.1X_C2.html)

An Introduction to 802.11i (Wikipedia)

[http://en.wikipedia.org/wiki/IEEE\\_802.11i-2004](http://en.wikipedia.org/wiki/IEEE_802.11i-2004)

Selecting an EAP Method – RADIUS Server Implications

<http://www.interlinknetworks.com/labels/802.1X.html>

### Standards Documents

IEEE 802.11i-2004 (Amendment to 802.11 to add WPA2)

<http://standards.ieee.org/getieee802/download/802.11i-2004.pdf>

IEEE 802.1X-2004 Standard

<http://www.ieee802.org/1/pages/802.1X-2004.html>

Internet Draft of the Microsoft Implementation of PEAP

<http://tools.ietf.org/html/draft-kamath-pppext-peapv0-00>

**Ruckus Wireless, Inc.**

880 West Maude Avenue, Suite 101, Sunnyvale, CA 94085 USA

(650) 265-4200 Ph \ (408) 738-2065 Fx

