Integrated Authentication Configuration Instructions for the EMS Web Client and EMS Campus Planning Interface

Dean Evans & Associates, Inc.
Integrated Authentication
Configuration Instructions
for the EMS Web Client
and EMS Campus Planning Interface

INTRODUCTION .................................................................................................................. 4
CUSTOMER SUPPORT .............................................................................................................. 4
EMS VERSION REQUIREMENTS ............................................................................................... 4
MANAGING EMS USERS ........................................................................................................... 4
INTEGRATED WINDOWS AUTHENTICATION .............................................................................. 4
  ACTIVATING INTEGRATED WINDOWS AUTHENTICATION FOR IIS 6.0 .......................... 4
  ACTIVATING INTEGRATED WINDOWS AUTHENTICATION FOR IIS 7 ............................... 5
LDAP AUTHENTICATION ......................................................................................................... 7
  OVERVIEW .......................................................................................................................... 7
  CONFIGURATION ............................................................................................................... 7
Introduction

The Integrated Authentication module is a component for the EMS Web Client and EMS Campus Planning Interface (EMS Campus only) that provides single-sign-on capability using Integrated Windows Authentication or LDAP. This document lists the steps you must take to configure these Integrated Authentication options. If you are unsure whether your organization is licensed for Integrated Authentication or you would like to learn more about it, please contact your Account Executive.

**Note:** For information on how to enable Integrated Authentication for Virtual EMS, please see the Integrated Configuration Instructions for Virtual EMS document.

Customer Support

Unlimited toll-free customer support is available to EMS users who have a current Annual Service Agreement (ASA). If you are unable to resolve a problem or answer a question by reading the EMS documentation, contact us at:

- **Email:** support@dea.com
- **Web:** www.dea.com
- **Phone:** (800) 288-4565
- **Fax:** (303) 796-7429

EMS Version Requirements

The latest version of EMS must be installed:

- EMS Workplace 6.0 or greater
- EMS Campus 3.0 or greater
- EMS Enterprise 6.0 or greater
- EMS Legal 6.0 or greater
- EMS District 6.0 or greater
- EMS Professional 12.0 or greater

Managing EMS Users

In order to access the EMS Web Client or EMS Campus Planning Interface, a user must have an active EMS User account. EMS User accounts are created by your EMS Administrator within EMS. For more information on how to create an EMS User account, please refer to the EMS Setup Guide.

**Important:** When creating an EMS User account in an Integrated Authentication environment, you must specify a value in the EMS User **Network ID** field.

Integrated Windows Authentication

**Overview**

Integrated Windows Authentication (IWA) is a built-in Microsoft Internet Information Services (IIS) authentication protocol that can be used to automatically authenticate and sign-in a user. Integrated Windows Authentication works only with Internet Explorer and is best used on intranets where all clients accessing the EMS Web Client/EMS Campus Planning Interface are within a single domain. For more information, please review the following Microsoft TechNet article on IWA.
When a domain user logged onto a networked PC hits the site, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID information recorded in the Network ID field of your EMS User records. If a match exists, the EMS User will be automatically logged-in.

**Activating Integrated Windows Authentication for IIS 6.0**

1. On the web server that hosts your EMS Web Client/EMS Campus Planning Interface site(s), open **IIS Manager**.
2. Locate your web site.

3. Right-click your site and choose **Properties**. The Properties screen will open.
4. Go to the **Directory Security** tab and click the **Edit** button under the **Authentication and access control** section. The Authentication Methods screen will open.
5. Uncheck the **Enable anonymous access** option. The **Integrated Windows authentication** option should be the only option checked.

6. Click **OK** to exit the Authentication Methods screen. Click **OK** again to exit the Properties screen. You have completed the necessary IIS configuration steps for IIS 6.0.
Activating Integrated Windows Authentication for IIS 7

1. On the web server that hosts your EMS Web Client/EMS Campus Planning Interface site(s), open **IIS Manager**.
2. Locate and highlight your web site.
3. Double-click the **Authentication** option in the **IIS** section.
4. Right-click the **Windows Authentication** option and select **Enable**.
5. Right-click the **Anonymous Authentication** option and select **Disable**.
6. You have completed the necessary IIS configuration steps for IIS 7.
LDAP Authentication

Overview
Lightweight Directory Access Protocol (LDAP) is an application protocol for querying directory information. The LDAP Authentication method provides single-sign-on capability using your organization’s LDAP environment and can be used in both intranet and internet deployments of the EMS Web Client and the EMS Campus Planning Interface.

When a user logs into the EMS Web Client or EMS Campus Planning Interface with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the Network ID field of your EMS User records. If a match exists, the User will be logged-in.

Configuration
The LDAP authentication configuration for the EMS Web Client and the EMS Campus Planning Interface occurs within Virtual EMS.

1. Log-into Virtual EMS with a Web User that belongs to a Web Security Template containing the Web Administrator role (Configuration > Web > Web Security Templates).
2. Redirect your browser to:
   
   [ServerName]/VirtualEMS/LDAPConfiguration.aspx (replace [ServerName] with the name of your web server)

4. Select the Authenticate users via LDAP checkbox to enable LDAP authentication.
5. **Use advanced communication options**: Skip this step for Active Directory environments. Enabling this checkbox requires that you complete the settings on the **Communication Options** tab.

6. In the **Path for LDAP Query** field, specify a valid LDAP path (example – LDAP://YourCompany.com)

7. **List of Domains**: Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.

8. In the **LDAP Domain\User** field, enter a Domain User account that has rights to query LDAP (example – YourDomain\User)

9. In the **Password** field, enter a valid Password for the User Account entered in the previous step.

10. Specify the appropriate LDAP **Authentication Type** for your environment.

    **Note**: The other tabs (Communication Options, Core Properties, Non-AD Config and LDAP Queries) should only be edited with assistance from our Support Department when special circumstances arise with unique configurations of LDAP.

11. Click **Save**.