Integrated Authentication Configuration Instructions For Virtual EMS

EMS Workplace 7.0
EMS Campus 4.0
EMS Enterprise 7.0
EMS Legal 7.0
EMS District 7.0
EMS Professional 13.0

Dean Evans and Associates LLC

Event Management Systems
Schedule Clarity

Copyright

Copyright © 2014 Dean Evans and Associates LLC All rights reserved.

No part of this document may be reproduced, transmitted or stored in a retrieval system in any form, electronic or mechanical, for purposes other than the personal use of the original purchaser except by written permission of Dean Evans and Associates LLC

Dean Evans and Associates LLC
6465 Greenwood Plaza Blvd
Suite 600
Centennial, CO 80111

This document may be copied for use by individuals employed by the purchaser.

Information in this document is subject to change without notice.

EMS, the EMS logo and EMS Regics are registered trademarks of Dean Evans and Associates LLC Event Management Systems, EMS Enterprise, EMS Professional, EMS Lite, EMS Campus, EMS Workplace, EMS Legal, EMS District, EMS Master Calendar and Virtual EMS are trademarks of Dean Evans and Associates LLC Microsoft, Windows and Outlook are registered trademarks and SQL Server is a trademark of Microsoft Corporation. Lotus Notes and Domino are registered trademarks of IBM Corporation. Other products, brands and trademarks are property of their respective owners/companies.

Integrated Authentication Configuration Instructions For Virtual EMS

© 2012 Dean Evans and Associates LLC

Introduction

The Integrated Authentication module is a component for Virtual EMS that provides single-sign-on capability using Integrated Windows Authentication, your organization's portal, or LDAP. This document lists the steps you must take to configure these Integrated Authentication options for Virtual EMS. 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 the EMS Web Client or the Campus Planning Interface, please see the *Integrated Configuration Instructions for the EMS Web Client* 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**

Managing Web Users

In order to make a reservation in Virtual EMS, a user must have an active Web User account with appropriate room request privileges. Several options exist to create Web User accounts within EMS.

New Web User Accounts

Manual Creation

Web User accounts can be created manually by EMS Administrators within EMS or by anonymous Web Users on Virtual EMS themselves. For information on how to create Web User accounts in EMS or how to configure Virtual EMS to allow anonymous Web Users to request an account, please refer to the *EMS Setup Guide*.

Important: When manually creating a Web User account in an Integrated Authentication environment, you must specify a value in the Web User **Network ID** field or the **External Reference** field. The ***Field Used to Authenticate Web User*** Virtual EMS Parameter (within *System Administration* > *Settings* > *Parameters (Virtual tab)*) is used by Virtual EMS to determine which value should be used for authentication.

HR Toolkit (for EMS Workplace, EMS Campus, EMS Enterprise, EMS District and EMS Legal only)

The HR Toolkit is an optional component that allows you to automate the creation and maintenance of Web User records in EMS using an outside employee data source like your HR system or another data store within your organization. Please refer to the *HR Toolkit Installation Instructions* for information. If you are not licensed for the HR Toolkit, but would like to learn more about it, please contact your Account Executive.

© 2012 Dean Evans and Associates LLC CONFIDENTIAL

Automatic Web User Account Creation

Various configuration settings are available to automatically create Web User records (and assign the appropriate Web Process Template(s) if applicable) when a user hits your Virtual EMS site for the first time. Within the Virtual EMS Parameters area of EMS (*System Administration* > *Settings* > *Parameters (Virtual tab)*), the following parameters must be set accordingly:

Area	Description	Value
Account Management	Auto Create Web User Account (for Integrated Authentication)	Yes
Account Management	Default Security Template for User	*Must be specified*
Account Management	Security Status for User	Active

For organizations using Portal authentication, EMS supports a simple account provisioning strategy. When using Auto Create, EMS requires that a web user account is provisioned with a name, an email address and a NetworkId (some authentication key), otherwise the user will be redirected to the Account Management page and be asked to manually enter the required information. In addition to the required fields, EMS also supports collecting phone, fax and an external reference value. The below parameters are meant to help create a more complete web user. The values for each of the parameters are to be determined by the information populated by your portal.

Area	Description	Value
Authentication	Portal Authentication Email Variable	*Must be specified*
Authentication	Portal Authentication External Reference Variable	*Must be specified*
Authentication	Portal Authentication Fax Variable	*Must be specified*
Authentication	Portal Authentication Name Variable	*Must be specified*
Authentication	Portal Authentication Phone Variable	*Must be specified*

EMS Workplace, EMS Campus, EMS Enterprise, EMS District, and EMS Legal customers are also able to assign default Web Process Templates when a new Web User account is created. To automatically assign a Web Process Template to new Web Users, select the ***Available to New Web Users*** option within your Web Process Template(s) (*Configuration* > *Web* > *Web Process Templates*).

In EMS Professional, the ***Default Security Template for User*** parameter shown above is used to assign the correct Web Process Template to new Web User records.

EMS customers using the LDAP Authentication method can use an alternate method to assign a Web Process Template to a Web User based on the LDAP Group(s) that that user belongs to. This approach can be used in addition to or in lieu of the Web Process Template assignment approach discussed above. Please see the LDAP Authentication section below for configuration instructions.

Existing Web User Accounts

© 2012 Dean Evans and Associates LLC

Warning for Existing EMS Customers: Before activating any Integrated Authentication option, the **Network ID** field or **External Reference** field must be populated on all existing Web User records. **Ignoring this step may result in duplicate Web User records.**

Integrated Windows Authentication

Overview

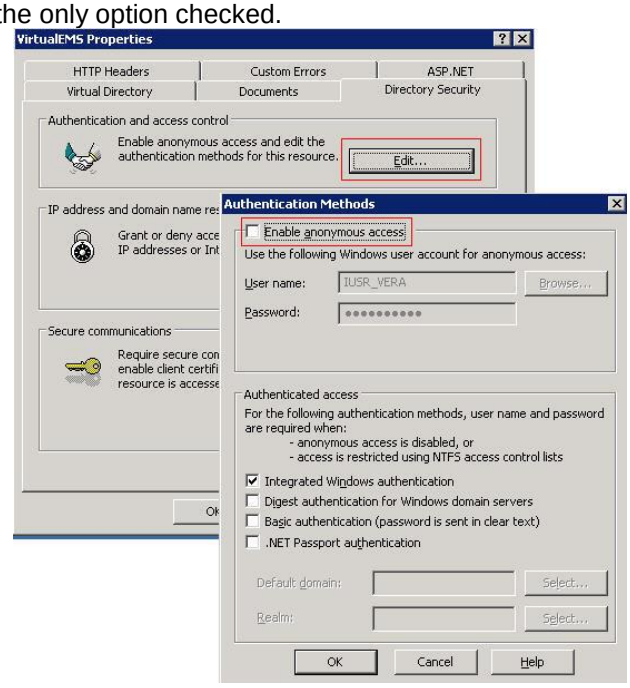
Integrated Windows Authentication (IWA) is a built-in Microsoft Internet Information Services (IIS) authentication protocol that can be used to automatically authenticate and sign-in a user to Virtual EMS. Integrated Windows Authentication works only with Internet Explorer and is best used on intranets where all clients accessing Virtual EMS 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 Virtual EMS site, their Active Directory credentials (Domain\User ID) are compared against corresponding Domain\User ID information recorded in the **Network ID** and\or **External Reference** fields of your EMS Web User records. If a match exists, the Web User will be automatically logged-into Virtual EMS.

Note: The ***Field Used to Authenticate Web User*** Virtual EMS Parameter (within *System Administration > Settings > Parameters (Virtual tab)*) is used by Virtual EMS to determine which value should be used for authentication.

Activating Integrated Windows Authentication for IIS 6.0

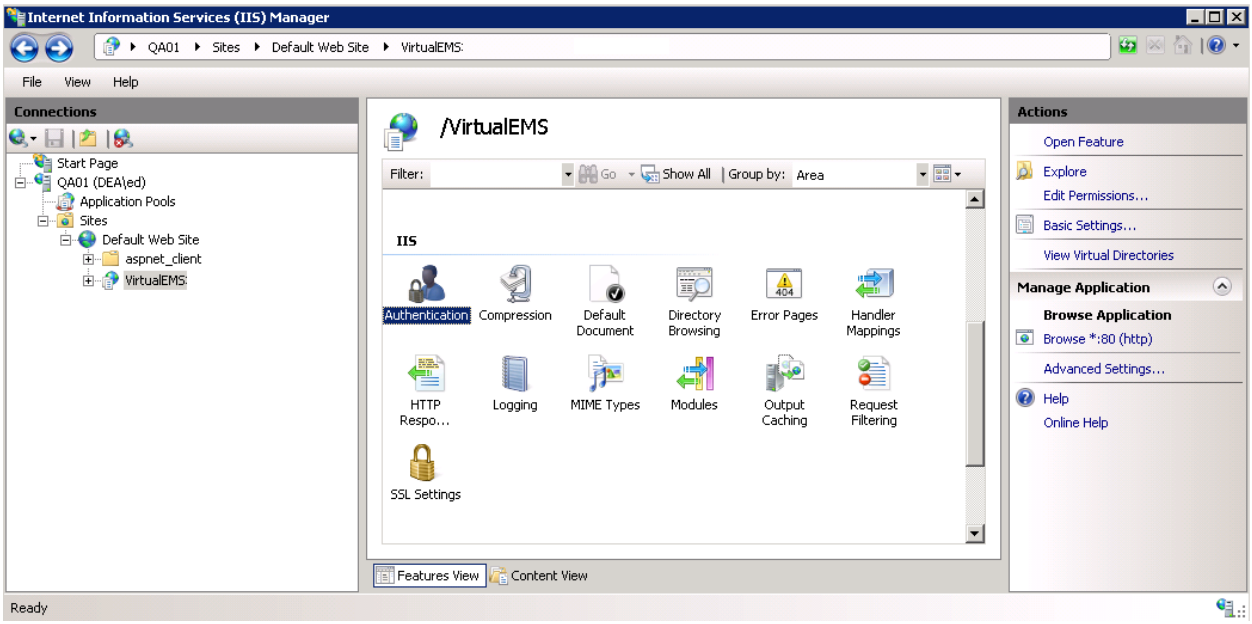
1. On the web server that hosts your Virtual EMS site, open **IIS Manager**.
2. Locate your Virtual EMS web site.
3. Right-click your Virtual EMS site and choose **Properties**. The Properties screen will open.
4. Go to the **Directory Security** tab and click the **Edit** button under the *Authentication 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.



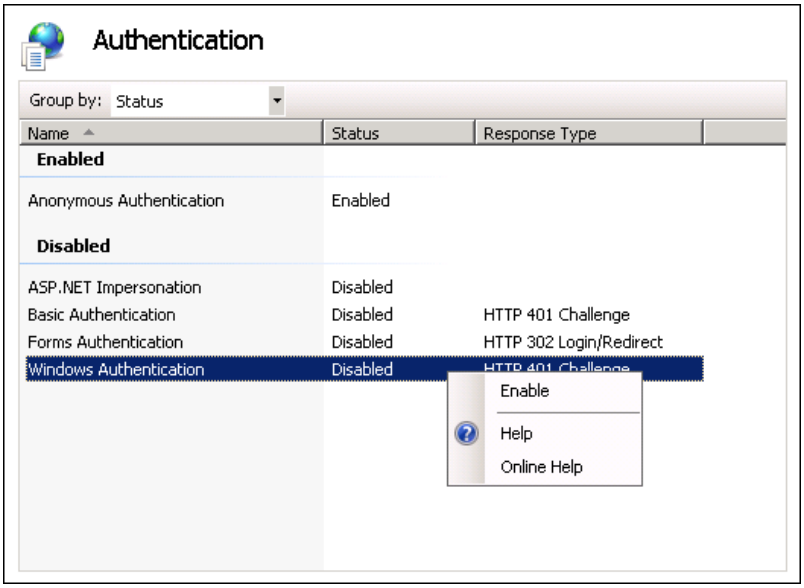
6. Click **OK** to exit the Authentication Methods screen. Click **OK** again to exit the Properties screen. You have completed the necessary IIS configuration steps for IIS 6.0.

Activating Integrated Windows Authentication for IIS 7

1. On the web server that hosts your Virtual EMS site, open **IIS Manager**.
2. Locate and highlight your Virtual EMS 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.

© 2012 Dean Evans and Associates LLC

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 Virtual EMS.

When a user logs-into Virtual EMS with their User ID and Password, their credentials are authenticated against LDAP and compared against corresponding user information recorded in the **Network ID** and/or **External Reference** fields of your EMS Web User records. If a match exists, the Web User will be logged-into Virtual EMS inheriting any Web Process Template rights that their LDAP Group has been assigned to.

Note: The Virtual EMS LDAP-Web Process Template assignment process requires that your implementation of LDAP stores group information (e.g. staff, student, department, etc.) as a Directory Service object containing a property (i.e. member) that contains the users that belong to your various groups.

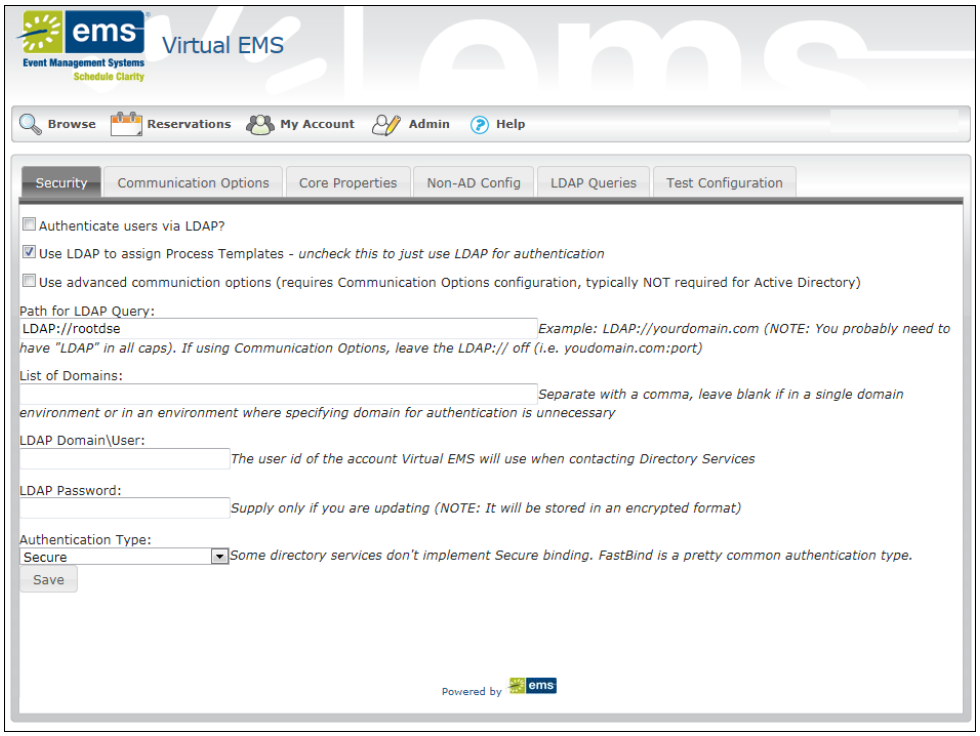
Note: The ***Field Used to Authenticate Web User*** Virtual EMS Parameter (within *System Administration > Settings > Parameters (Virtual tab)*) is used by Virtual EMS to determine which value should be used for authentication.

Configuration

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:

   http://[ServerName]/ VirtualEMS/LDAPConfiguration.aspx (replace [ServerName] with the name of your web server)

© 2012 Dean Evans and Associates LLC



3. Go to the **Security** tab.
4. Select the **Authenticate users via LDAP** checkbox to enable LDAP authentication.
5. Select the **Use LDAP to assign Process Templates** checkbox if LDAP will be used to assign Web Process Templates to your Web Users.
6. **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.
7. In the **Path for LDAP Query** field, specify a valid LDAP path (example – LDAP://YourCompany.com)
8. **List of Domains**: Skip this step if your organization uses a single domain. Otherwise, provide a comma separated list of your domains.
9. In the **LDAP Domain\User** field, enter a Domain User account that has rights to query LDAP (example – YourDomain\User)
10. In the **Password** field, enter a valid Password for the User Account entered in the previous step.
11. 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.

12. Click **Save**.

    Note: If you want Web Users to inherit Web Process Templates based on the LDAP Group(s) they belong to, proceed to Step #13. Otherwise, you have completed the configuration process.

13. Within EMS, go to the Web Process Templates area (*Configuration* > *Web* > *Web Process Templates*).
14. Within a Web Process Template, locate the **LDAP Groups** tab and map the appropriate LDAP Group(s) to that Web Process Template.
15. Click **OK**.

© 2012 Dean Evans and Associates LLC

Portal Authentication

Overview

The Portal Authentication method provides Virtual EMS single sign-on capability using your organization's portal (e.g. SiteMinder, Plumtree, uPortal, etc.). When a user logged into your portal accesses Virtual EMS, a predefined user-specific variable (e.g. email address, employee/student ID, network ID, etc.) captured by your portal/sign-on page is compared against corresponding information recorded in the **Network ID and**/or **External Reference** fields of your EMS Web User records. If a match exists, the Web User will be automatically logged-into Virtual EMS.

Note: The ***Field Used to Authenticate Web User*** Virtual EMS Parameter (within *System Administration > Settings > Parameters (Virtual tab)*) is used by Virtual EMS to determine which value should be used for authentication.

Several built-in authentication methods to pass-in credentials are available including:

- Server Variable (Header Variable)
- Session
- Form
- Cookie
- Query String
- Federated (SAML)

For a more detailed explanation of the authentication methods outlined above, please see the Appendix.

Installation/Configuration

1. Within the Virtual EMS Parameters area of EMS (*System Administration > Settings > Parameters (Virtual tab)*), the following parameters must be set accordingly:

Area	Description	Value
Authentication	Portal Authentication Cookie Key	Required if Portal Authentication Method = Cookie
Authentication	Portal Authentication Method	Server Variable Session Form Cookie Query String
Authentication	Portal Authentication Variable	User variable to be compared against the EMS Web User **External Reference/Network ID** field

2. Direct users to the default Virtual EMS page:

   (http://[ServerName]/ VirtualEMS/Default.aspx (replace [ServerName] with the name of your web server)

Appendix

Portal Authentication Methods

Server Variable Method (Header Variable)

Server Variable/Header Variable is a collection of variables that are set by Internet Information Server (IIS). Applications like SiteMinder create custom server variables for portal site use.

Code example:
Set the **Portal Authentication Method** parameter to *Server Variable* and type the appropriate variable for the **Portal Authentication Variable** parameter. Direct users to your Virtual EMS Default.aspx page.

Server Variable Method – Federated (SAML)

SAML can be leveraged for authentication with your EMS applications by leveraging our portal authentication method and a service provider of your choosing.

Method 1: Locally installed Service Provider

Using this method, you install a service provider of choice on the webserver hosting the EMS web applications. All traffic is routed through that service provider (typically via an ISAPI filter). This service provider will manage all of the authentication for the user. Once the user has successfully authenticated it will pass an identifier for the user to the EMS application using one of our portal methods. In this scenario typically the Server Variable (Header) method is used.

Steps to Configure

1. Install and configure a service provider on the EMS web server
2. Set the service provider to protect the specified EMS web applications
3. Configure the service provider to pass the required user attributes
4. In EMS configure the VEMS parameter “Portal Authentication Method”
5. In EMS configure the applicable Portal Authentication Variables.

Method 2: Remote Service Provider

This method can be common if there is already a server configured with a service provider in your environment, handling authentication for other applications. In EMS you can configure your application to re-direct any login requests to the other server to be authenticated. Once the user is authenticated, the server with your service provider installed sends the user back to the EMS Application with an identifier for the user in the header, or within a cookie. The EMS application reads this header, or cookie value, and leverages portal authentication to sign the user in with the matched credentials.

Steps to Configure

1. Install and configure a service provider on the EMS web server
2. Set the service provider to protect the specified EMS web applications
3. Configure the service provider to pass the required user attributes
4. In EMS configure the VEMS parameter “Portal Authentication Method”
5. In EMS configure the applicable Portal Authentication Variables.
6. In EMS Change the Login URL under Configuration>Web>Web Menus
    a. Select Login.aspx, Click Edit
    b. Enter in the URL to your Remote Service Provider
7. Configure your remote Service provider to send the user back to the default.aspx page of the web application that the request originated from.

© 2012 Dean Evans and Associates LLC

EMS Configuration

Please reference our Portal Authentication section for further details around the configuration required within EMS. There are a number of different options available. You will need to know the method that the user identifying value will be passed and the name of that value. Other values can also be passed (ie: email address and phone number) to aid in automatic web user account provisioning as well.

Session Method

A session is a way to provide/maintain user state information in an inherently stateless environment. It provides access to a session-wide cache you can use to store information.

In order to use the session method, set the **Portal Authentication Method** parameter to *Session* and type the appropriate variable for the **Portal Authentication Variable** parameter. Then you must create an asp.net web page and name it with the .aspx extension similar to the example below. The asp.net web page created must be copied into the Virtual EMS root web directory. It must be copied there in order for Virtual EMS to read the session variable.

You will need to pass through the user's email address or external reference to your asp.net web page.

Code example in vb.net:

```
<%@ Import Namespace="System" %>
<script runat="server" language="vb">
        Sub Page_Load(ByVal sender As System.Object, ByVal e As System.EventArgs)
                Session.Item("VEMSSession") = "test@dea.com"
                Response.Redirect("Default.aspx")
        End Sub
</script>
```

Form Method

Forms enable client-side users to submit data to a server in a standardized format via HTML. The creator of a form designs the form to collect the required data using a variety of controls, such as INPUT or SELECT. Users viewing the form fill in the data and then click Submit to send the data to the server.

To use the form method, set the **Portal Authentication Method** parameter to *Form* and type the appropriate variable for the **Portal Authentication Variable** parameter. To create portals through a form, create a web page with a form similar to below. Once the user logs on through the portal, the form below can be submitted to log the user on to Virtual EMS.

Code example in HTML:

```
<Form name="form1" method="Post" action=" http://[ServerName]/ VirtualEMS/Default.aspx ">
        <input type="hidden" id="VEMSFORM" name="VEMSFORM" value="test@dea.com">
        <input type="submit" value="submit">
</form>
```

Cookie Method

A cookie is a small piece of information stored by the browser. Each cookie is stored in a name/value pair called a crumb—that is, if the cookie name is "id" and you want to save the id's value as "this", the cookie would be saved as id=this.

You can store up to 20 name/value pairs in a cookie, and the cookie is always returned as a string of all the cookies that apply to the page. This means that you must parse the string returned to find the values of individual cookies. Cookies accumulate each time the property is set. If you try to set more than one cookie with a single call to the property, only the first cookie in the list will be retained.

To use the cookie method, set the **Portal Authentication Method** parameter to *Cookie* and type the appropriate variable for the **Portal Authentication Cookie Key** parameter. Then create a web page with code similar to below. Once the user logs on through the portal, take their user logon information and create a cookie. After the cookie is created send the user to your Virtual EMS Default.aspx page.

Code example in Active Server Pages 2.0:

```
<%@LANGUAGE="VBSCRIPT" %>
<%
        Response.Expires = -1
        Response.Cookies("VEMSCookie")("CookVal") = "test@dea.com"
        Response.Cookies("VEMSCookie").Path = "/"
        Response.Cookies("VEMSCookie").Expires = DateAdd("m", 3, Now)
        Response.Redirect("http://[ServerName]/ VirtualEMS/Default.aspx ")
%>
```

Query String Method

A query string is information appended to the end of a page's URL. An example using portal authentication is below

Code example:

http://[ServerName]/ VirtualEMS/Default.aspx?MCQS=test@dea.com

To use the query string method, set the **Portal Authentication Method** parameter to *Query String* and type the appropriate variable for the **Portal Authentication Variable** parameter.

© 2012 Dean Evans and Associates LLC