Plan-a-Meeting (PAM) Installation Instructions

For Microsoft Exchange® Integration

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 & Associates, Inc.

Event Management Systems
Schedule Clarity

Copyright

Dean Evans & Associates, Inc.
6465 Greenwood Plaza Blvd
Suite 600
Centennial, CO 80111

Plan-a-Meeting (PAM)
Installation Instructions
For Microsoft Exchange

Introduction

Plan-a-Meeting (PAM) is a component for Virtual EMS that integrates with Microsoft Exchange or IBM Lotus Notes (EMS Workplace/Enterprise only). With this module, web users can view the availability of both meeting rooms *and* attendees, and send Microsoft Outlook or IBM Lotus Notes-compatible meeting invitations - all from within Virtual EMS.

This document lists the steps you must take to install the PAM component for Virtual EMS. You must be licensed for EMS, Virtual EMS, and PAM in order to configure and use this module. If you are unsure if your organization is licensed for PAM, or if you would like to learn more about it, please contact your Account Executive.

Customer Support

Unlimited toll-free customer support is available to EMS users who have a current Annual Service Agreement (ASA). Before you begin the installation/configuration process, we recommend that you contact Customer Support (or a member of the Professional Services group if you are working with one) to discuss the PAM setup process in your IIS and Microsoft Exchange or IBM Lotus Domino environment.

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

Plan-a-Meeting Requirements

- **EMS/Virtual EMS Installed**
  EMS and Virtual EMS must be installed and operational.

- **Valid PAM License**
  You must be licensed for EMS, Virtual EMS, and PAM in order to configure and use this module. If you are unsure if your organization is licensed for PAM, or if you would like to learn more about it, please contact your Account Executive.

- **Web Server Requirements**
  - The PAM Web Service is typically installed on the web server that hosts your Virtual EMS web site. The system requirements for the PAM Web Service are similar to the Virtual EMS requirements listed on www.dea.com.

  - **Microsoft .NET Framework 3.5**

  - The PAM Web Service must be reachable via http(s) by all EMS components (i.e. EMS desktop application, Virtual EMS, EMS Web Client and EMS for Outlook if applicable). The PAM Web Service must also be able to reach your Microsoft Exchange environment.

- **Microsoft Exchange**
  Microsoft Exchange 2000, 2003 (SP2), 2007 (SP1) or 2010 is required.

  IMPORTANT: Multi-tenant Microsoft Exchange Hosted Services environments may not be compatible with PAM. Please contact your Professional Services Consultant if your organization utilizes Microsoft Exchange Hosted Services.

  Microsoft Exchange 2000/2003

- Web Access (OWA) must be enabled. A valid OWA URL will be required during configuration (example – https://mail.YourCompany.com/exchange/)

- Exchange public folder access must be enabled. A valid OWA public folder URL will be required during configuration (example – https://mail.YourCompany.com/public/)

- LDAP URL. A valid LDAP URL will be required during configuration (example – LDAP://YourCompany.com)

- Microsoft Exchange Mailbox Store Account (PAM Account). An account with Full Access permissions for all mailboxes in your Exchange mailbox store is required. This account must also have access to query LDAP. It is recommended that you create a new account to be specifically used by PAM instead of re-using an existing account. Once inputted, the PAM account's password is encrypted using 3DES technology and is not redisplayed to any user, including EMS administrators.

  Important: Plan-a-Meeting configuration issues often relate to access rights with this account. Please ensure that the account has the necessary Full Access permissions.

Microsoft Exchange 2007/2010

- Exchange Web Services must be enabled.

- The Exchange Autodiscover service must be enabled.

Microsoft Exchange Impersonation Account (PAM Account). A **mail-enabled** account with Exchange Impersonation access to all mailboxes in your Exchange mailbox store is required (http://msdn.microsoft.com/en-us/library/bb204095(EXCHG.80).aspx or http://msdn.microsoft.com/en-us/library/bb204095.aspx). It is recommended that you create a new account to be specifically used by PAM instead of re-using an existing account. The PAM Web Service is able to utilize the PAM Account (created in Exchange) in either of the following ways:

- **Enter the credentials on the PAM Config page:** Once inputted, the PAM account's password is encrypted using 3DES technology and is not redisplayed to any user, including EMS administrators.
- **Use Application Pool identity when authenticating:** Create a new Application Pool in IIS Manager with the identity of your PAM account. The credentials are never stored in the EMS database. This process is covered in more detail in the Additional Information section below.

- **Note:** Microsoft Exchange Impersonation ONLY works via the Exchange Web Services Managed API. This means that although the PAM Account is able to act on behalf of other users in your organization, it can only be used in the context of an Exchange Web Services call; it will not work through Microsoft Outlook, OWA or any other Exchange client.

  Important: Plan-a-Meeting configuration issues often relate to access rights with this account. Please ensure that the account has the necessary permissions.

Mixed Mode Microsoft Exchange 2007/2010 and Microsoft Exchange 2000/2003

- Please see the requirements outlined above for each environment.

  Important: The PAM Account will require Full Access permissions for user mailboxes in your Exchange 2000/2003 mailbox store **AND** Exchange Impersonation access for user mailboxes in your Exchange 2007/2010 mailbox store.

Obtaining the Latest Release of the PAM Web Service

The latest release of the PAM Web Service can be downloaded from the online Support Center.

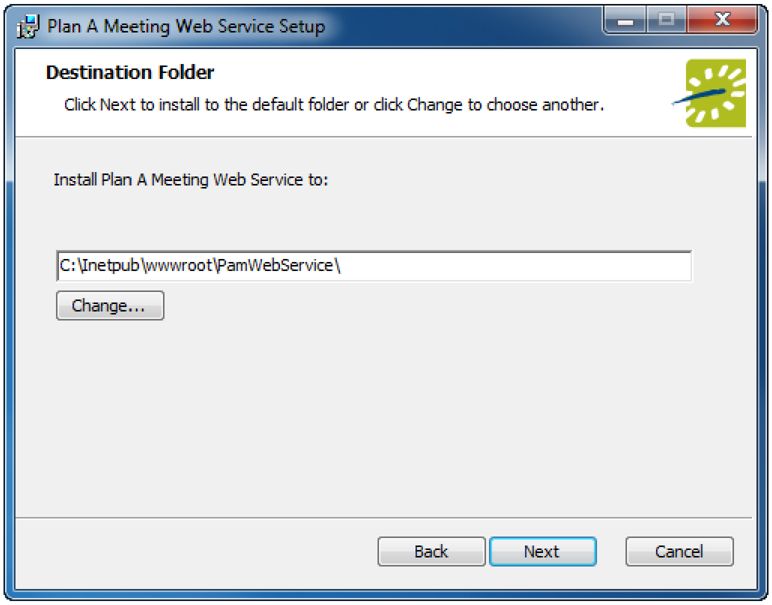
1. Go to www.dea.com and enter your Email Address and Password in the Support Center area.
2. Click the Software downloads link.
3. Download **PAM Web Service (PAMWebService.msi)**. Required for both first time installations and upgrades.

Installing/Upgrading the PAM Web Service

Important: Before beginning the installation process, please do the following:

- Install or upgrade your EMS databases as outlined in the *EMS Installation Instructions*.
- Manually **uninstall** any previous versions of the PAM Web Service on your web server.

1. Verify that the requirements outlined in the Plan-a-Meeting Requirements section have been met.
2. Download **PAMWebService.msi** onto the web server that will be running the PAM Web Service.
3. Run **PAMWebService.msi**.
4. The first screen welcomes you to the Plan A Meeting Web Service Setup Wizard. Click **Next** to begin the installation process. The *Destination Folder* screen will appear.



Plan A Meeting Web Service Setup

Destination Folder

Click Next to install to the default folder or click Change to choose another.

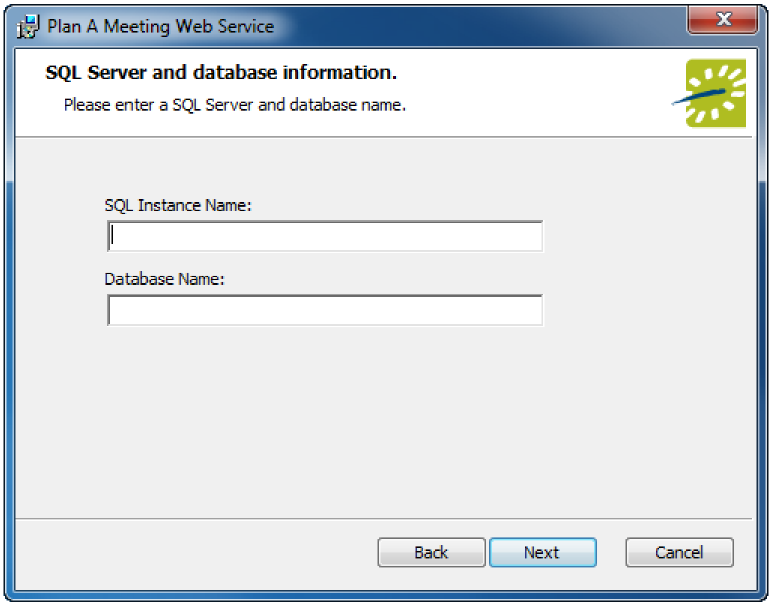
Install Plan A Meeting Web Service to:

C:\Inetpub\wwwroot\PamWebService\

5. Select the destination folder. The installation process will create a new physical directory on your web server based on the destination folder path entered ("PamWebService" in the example above.) Click **Next**.

   Note: The PAM Web Service should not be installed in the same physical directory as other EMS web-based products.

6. The *SQL Server and database information* screen will appear.



Plan A Meeting Web Service

SQL Server and database information.

Please enter a SQL Server and database name.

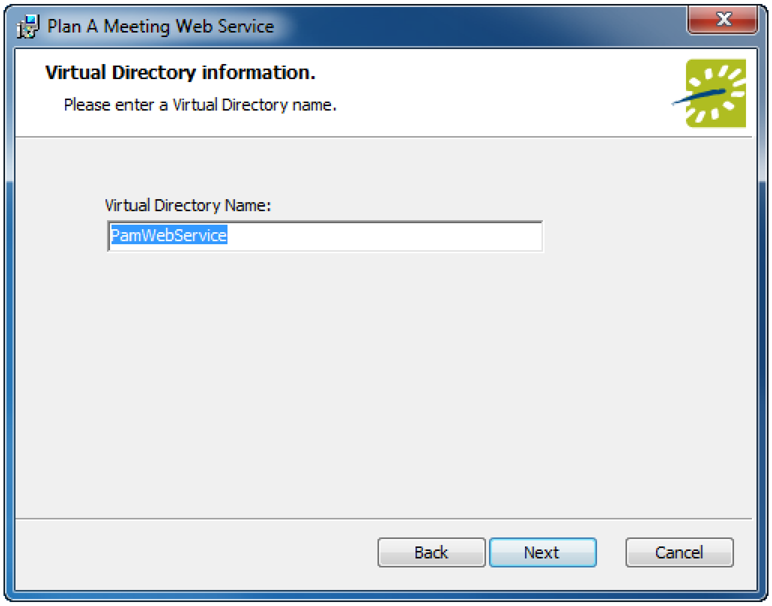
SQL Instance Name:

Database Name:

7. Enter your EMS SQL Instance Name.
8. Enter your EMS Database Name:

- EMS Professional and EMS Lite customers – enter “EMSData”
- EMS Workplace, EMS Campus, EMS Legal, EMS District, and EMS Enterprise customers – typically named “EMS”

9. Click **Next**.
10. The *Virtual Directory information* screen will appear.



Plan A Meeting Web Service

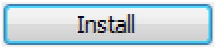
Virtual Directory information.

Please enter a Virtual Directory name.

Virtual Directory Name: PamWebService

11. The Virtual Directory Name will default to the destination folder specified in Step 5. It is recommended that you keep the default setting. The installation process will create a virtual directory on your web server based on the virtual directory entered (“PamWebService” in the example above.) Click **Next**.

Note: The PAM Web Service should not be installed in the same virtual directory as other EMS web-based products.

12. The *Ready to install Plan A Meeting Web Service* screen will appear. Click  to install the PAM Web Service.
13. The *Completed the Plan A Meeting Web Service Setup Wizard* screen will appear. Click **Finish**.
14. After following the steps above, verify your installation by opening a browser and entering the following:

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

    Important: The Service.asmx page must be run under anonymous access **without** any authentication methods in place (e.g. Integrated Windows Authentication or Portal).

Configuring PAM

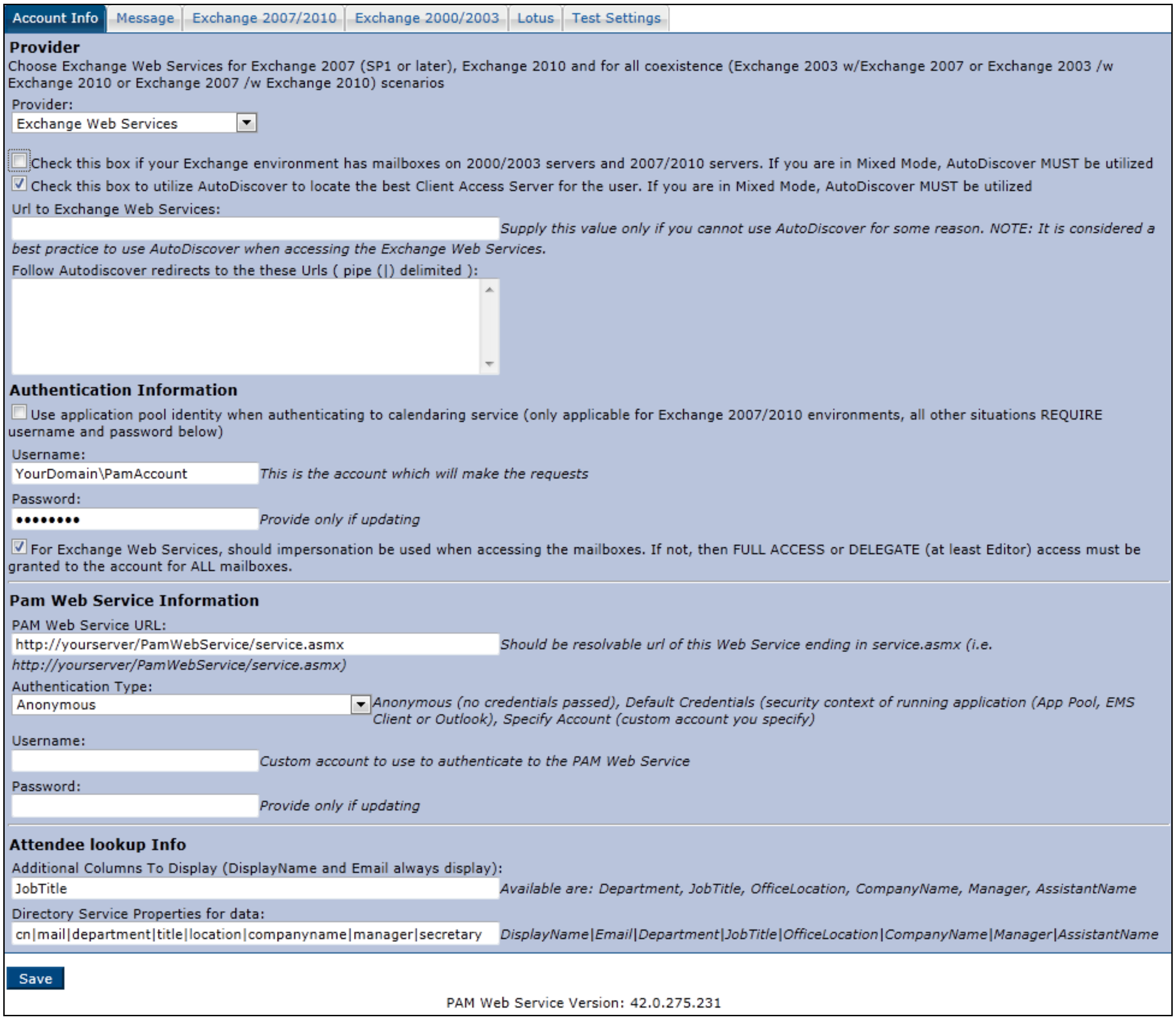
Required Settings for Exchange 2000/2003 OR Exchange 2007/2010 Environments

Note: For instructions on how to configure PAM for Mixed Mode environments, please see the Required Settings for Mixed Mode - Exchange 2000/2003 AND Exchange 2007/2010 Environments section below.

1. After following the steps above, access the PAM configuration area by opening a browser and entering the following:

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

2. Go the **Account Info** tab.



Provider

Choose Exchange Web Services for Exchange 2007 (SP1 or later), Exchange 2010 and for all coexistence (Exchange 2003 w/Exchange 2007 or Exchange 2003 /w Exchange 2010 or Exchange 2007 /w Exchange 2010) scenarios

Provider: Exchange Web Services

□ Check this box if your Exchange environment has mailboxes on 2000/2003 servers and 2007/2010 servers. If you are in Mixed Mode, AutoDiscover MUST be utilized

☑ Check this box to utilize AutoDiscover to locate the best Client Access Server for the user. If you are in Mixed Mode, AutoDiscover MUST be utilized

Url to Exchange Web Services: *Supply this value only if you cannot use AutoDiscover for some reason. NOTE: It is considered a best practice to use AutoDiscover when accessing the Exchange Web Services.*

Follow Autodiscover redirects to the these Urls (pipe (|) delimited):

Authentication Information

□ Use application pool identity when authenticating to calendaring service (only applicable for Exchange 2007/2010 environments, all other situations REQUIRE username and password below)

Username: YourDomain\PamAccount *This is the account which will make the requests*

Password: •••••••• *Provide only if updating*

☑ For Exchange Web Services, should impersonation be used when accessing the mailboxes. If not, then FULL ACCESS or DELEGATE (at least Editor) access must be granted to the account for ALL mailboxes.

Pam Web Service Information

PAM Web Service URL: http://yourserver/PamWebService/service.asmx *Should be resolvable url of this Web Service ending in service.asmx (i.e. http://yourserver/PamWebService/service.asmx)*

Authentication Type: Anonymous *Anonymous (no credentials passed), Default Credentials (security context of running application (App Pool, EMS Client or Outlook), Specify Account (custom account you specify)*

Username: *Custom account to use to authenticate to the PAM Web Service*

Password: *Provide only if updating*

Attendee lookup Info

Additional Columns To Display (DisplayName and Email always display): JobTitle *Available are: Department, JobTitle, OfficeLocation, CompanyName, Manager, AssistantName*

Directory Service Properties for data: cn|mail|department|title|location|companyname|manager|secretary *DisplayName|Email|Department|JobTitle|OfficeLocation|CompanyName|Manager|AssistantName*

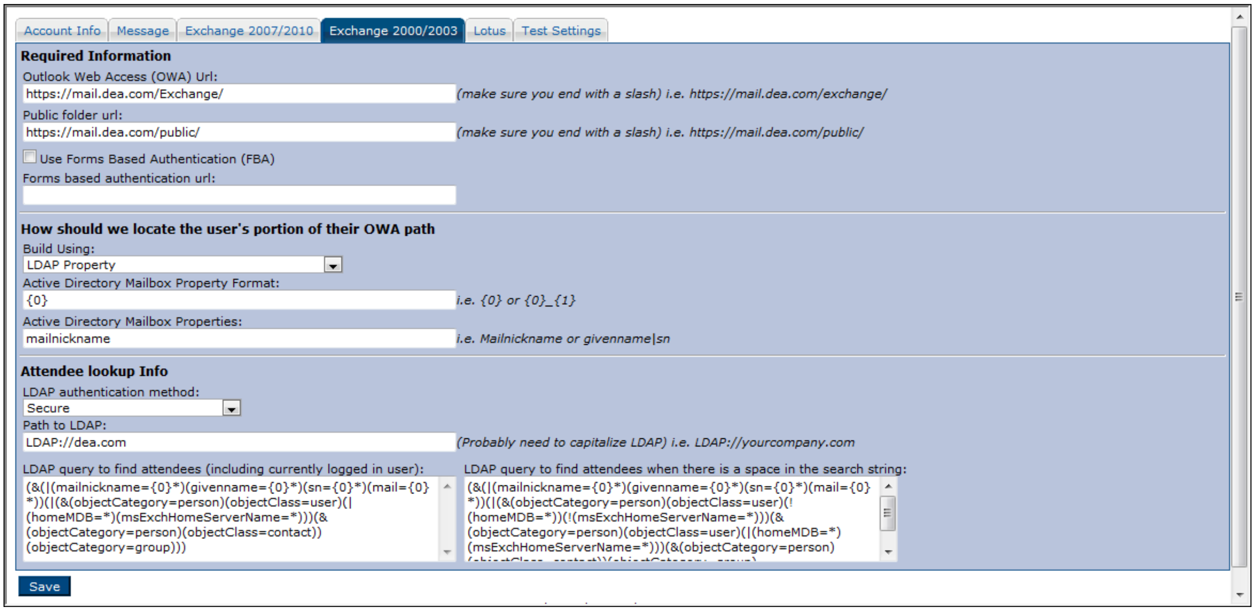
Save

PAM Web Service Version: 42.0.275.231

3. Select your email system in the **Provider** dropdown using the instructions provided on the page.
4. Check the box ".. utilize AutoDiscover to locate the best Client Access Server for the user…" Note: if you do not check this box, you **MUST** fill in the *Url to Exchange Web Services* field. This option requires the latest patch (79 or greater) and build of PAM Web Service to be installed.
5. Within the *Authentication Information* section, enter your PAM Account **User Name** and **Password**. The User Name should be prefixed with your domain (example – YourDomain\PAM Account.)
6. *(Optional)* The "Use application pool identity…" option allows you to set the PAM Account credentials at the Application Pool level instead of storing the credentials in the EMS database. See the Additional Information section below for more information about this option. If this option is selected, you **must** check the box to use Impersonation.
7. If you selected "Exchange Web Services" as your **Provider**, select the checkbox if the account specified has Exchange Impersonation access to all mailboxes in your Exchange mailbox store.
8. The PAM Web Service URL will be used in the EMS Configuration section later in this document.
9. Select the Authentication Type:
   - *Anonymous* – No authentication

- *Specify Account* – Relies on a custom account (not the PAM Account) that you create and manage. Please contact Customer Support (or a member of the Professional Services group if you are working with one) to discuss the configuration process for this option.
- *Default Credentials* – Relies on security context of EMS application calling the PAM Web Service. If using this option, Integrated Windows Authentication should be enabled for the PAM Web Service.

10. For MS Exchange 2007/2010 environments, click **Save**. Go to **step 14**.
11. For MS Exchange 2000/2003 environments, go the **Exchange 2000/2003** tab.



Required Information

Outlook Web Access (OWA) Url: https://mail.dea.com/Exchange/ *(make sure you end with a slash) i.e. https://mail.dea.com/exchange/*

Public folder url: https://mail.dea.com/public/ *(make sure you end with a slash) i.e. https://mail.dea.com/public/*

□ Use Forms Based Authentication (FBA)

Forms based authentication url:

How should we locate the user's portion of their OWA path

Build Using: LDAP Property

Active Directory Mailbox Property Format: {0} *i.e. {0} or {0}_{1}*

Active Directory Mailbox Properties: mailnickname *i.e. Mailnickname or givenname|sn*

Attendee lookup Info

LDAP authentication method: Secure

Path to LDAP: LDAP://dea.com *(Probably need to capitalize LDAP) i.e. LDAP://yourcompany.com*

LDAP query to find attendees (including currently logged in user):

```
(&(|(mailnickname={0}*)(givenname={0}*)(sn={0}*)(mail={0}
*))(|(&(objectCategory=person)(objectClass=user)(|
(homeMDB=*)(msExchHomeServerName=*)))(&
(objectCategory=person)(objectClass=contact))
(objectCategory=group)))
```

LDAP query to find attendees when there is a space in the search string:

```
(&(|(mailnickname={0}*)(givenname={0}*)(sn={0}*)(mail={0}
*))(|(&(objectCategory=person)(objectClass=user)(!
(homeMDB=*))(!(msExchHomeServerName=*)))(&
(objectCategory=person)(objectClass=user)(|(homeMDB=*)
(msExchHomeServerName=*)))(&(objectCategory=person)
```

12. Enter your **Outlook Web Access (OWA) UR**L (example – https://mail.YourCompany.com/exchange/)
13. Enter your **Public Folder URL** (example – https://mail.YourCompany.com/public/)
14. Check the **Use Forms Based Authentication (FBA**) checkbox if FBA is enabled in your environment. Specify the **Forms based authentication url**.
15. Enter your **Path to LDAP** (example – LDAP://YourCompany.com)

    Note: The default settings within the *How should we locate the user's portion of their OWA path* area are appropriate for the majority of installations. For more information about these settings, please see the Optional Settings section.

16. Click **Save**.
17. Go to the **Test Settings** tab.
18. In the **Test Email** field, enter a fully qualified email address (example - John.Smith@YourCompany.com).

    Note: When testing PAM, the email account that is being used (either on the Test Settings tab or in the Testing PAM section below) MUST exist in the Exchange environment being tested. If you are testing PAM in a development environment please verify that a mailbox for the email being used exists in that domain/environment.

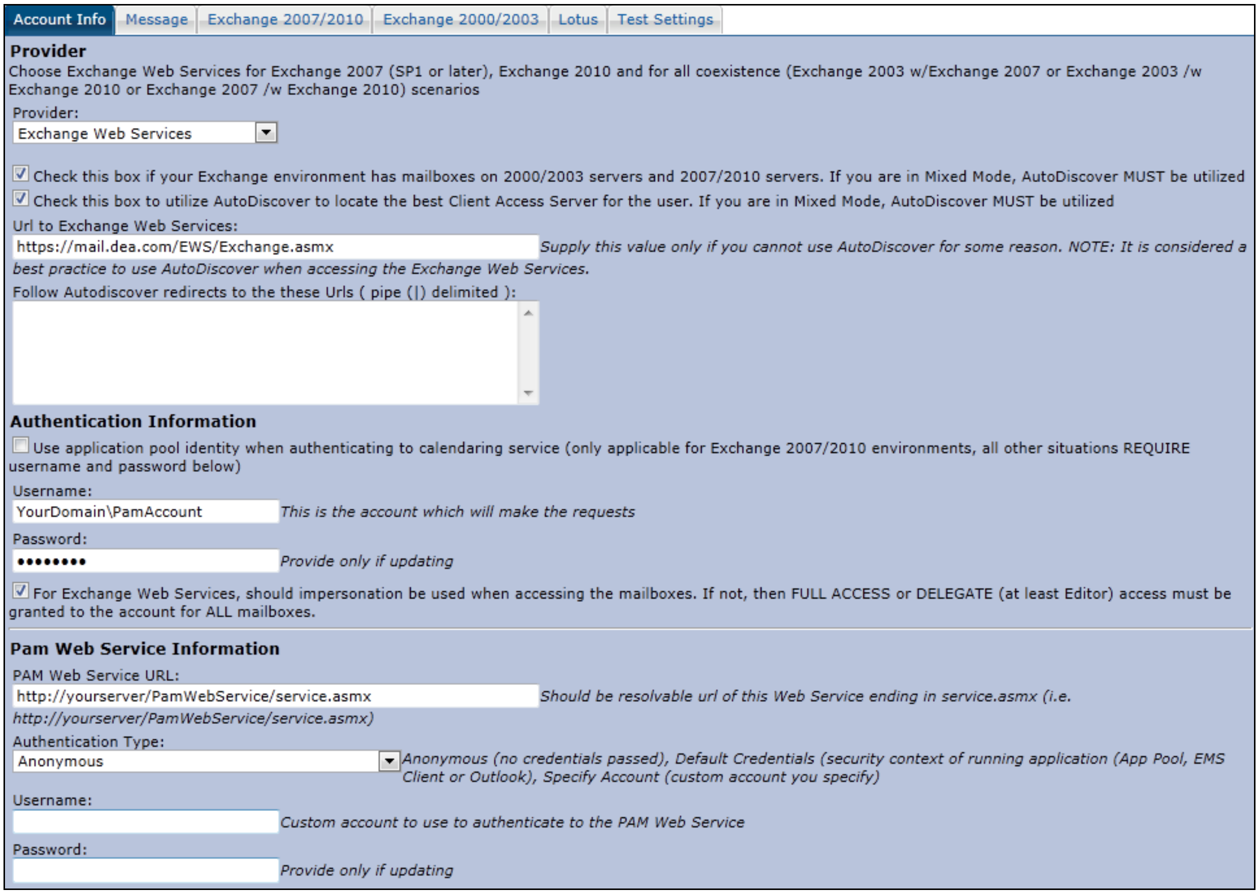
19. Click **Test Configuration**. If any errors are encountered, please verify your configuration. Otherwise, your PAM configuration is complete. Please go to the EMS Configuration section below.

Required Settings for Mixed Mode - Exchange 2000/2003 AND Exchange 2007/2010 Environments

1. After following the steps above, access the PAM configuration area by opening a browser and entering the following:

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

2. Go the **Account Info** tab.



Provider

Choose Exchange Web Services for Exchange 2007 (SP1 or later), Exchange 2010 and for all coexistence (Exchange 2003 w/Exchange 2007 or Exchange 2003 /w Exchange 2010 or Exchange 2007 /w Exchange 2010) scenarios

Provider: Exchange Web Services

☑ Check this box if your Exchange environment has mailboxes on 2000/2003 servers and 2007/2010 servers. If you are in Mixed Mode, AutoDiscover MUST be utilized

☑ Check this box to utilize AutoDiscover to locate the best Client Access Server for the user. If you are in Mixed Mode, AutoDiscover MUST be utilized

Url to Exchange Web Services: https://mail.dea.com/EWS/Exchange.asmx *Supply this value only if you cannot use AutoDiscover for some reason. NOTE: It is considered a best practice to use AutoDiscover when accessing the Exchange Web Services.*

Follow Autodiscover redirects to the these Urls (pipe (|) delimited):

Authentication Information

☐ Use application pool identity when authenticating to calendaring service (only applicable for Exchange 2007/2010 environments, all other situations REQUIRE username and password below)

Username: YourDomain\PamAccount *This is the account which will make the requests*

Password: •••••••• *Provide only if updating*

☑ For Exchange Web Services, should impersonation be used when accessing the mailboxes. If not, then FULL ACCESS or DELEGATE (at least Editor) access must be granted to the account for ALL mailboxes.

Pam Web Service Information

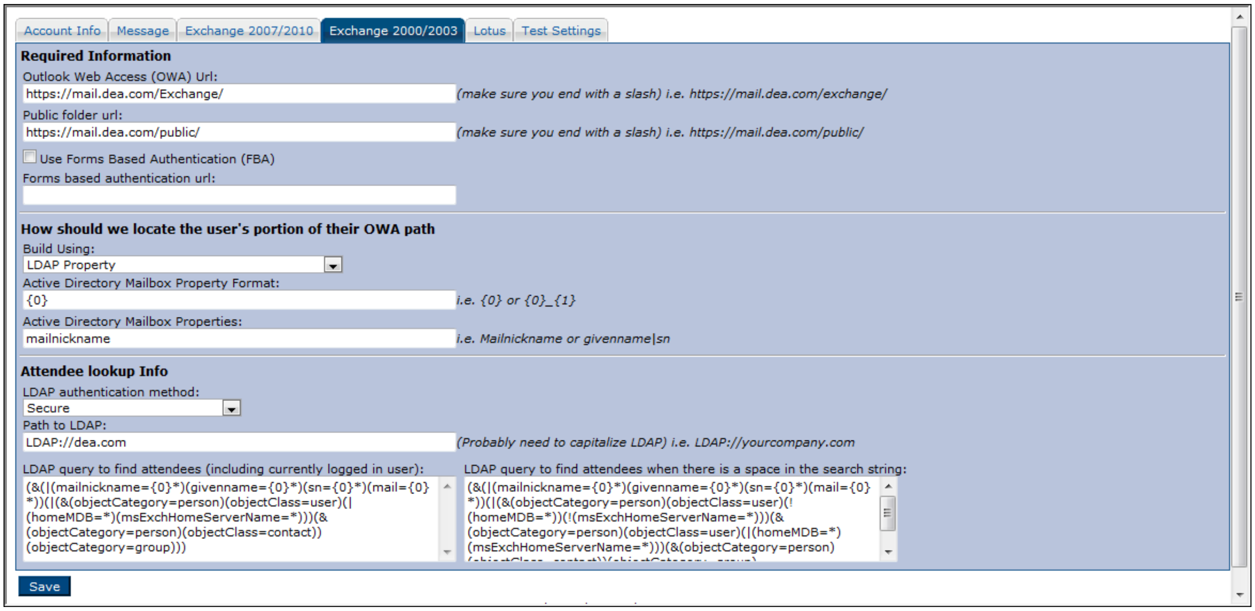
PAM Web Service URL: http://yourserver/PamWebService/service.asmx *Should be resolvable url of this Web Service ending in service.asmx (i.e. http://yourserver/PamWebService/service.asmx)*

Authentication Type: Anonymous *Anonymous (no credentials passed), Default Credentials (security context of running application (App Pool, EMS Client or Outlook), Specify Account (custom account you specify)*

Username: *Custom account to use to authenticate to the PAM Web Service*

Password: *Provide only if updating*

3. Select ‘Exchange Web Services’ in the **Provider** dropdown.
4. Check the box “.. if your Exchange environment has mailboxes on 200/2003 servers **and** 2007/2010 servers…”
5. Check the box “.. utilize AutoDiscover to locate the best Client Access Server for the user…” Note: the options in Steps 4 and 5 require the latest patch (79 or greater) and build of PAM Web Service to be installed. If you are using Mixed Mode, you must also use AutoDiscovery.
6. Within the *Authentication Information* section, enter your PAM Account **User Name** and **Password**. The User Name should be prefixed with your domain (example – YourDomain\PAM Account.)
7. Select the checkbox if the account specified has Exchange Impersonation access to all mailboxes in your Exchange 2007/2010 mailbox store.
8. The PAM Web Service URL will be used in the EMS Configuration section later in this document.
9. Go to the **Exchange 2000/2003** tab.



Required Information

Outlook Web Access (OWA) Url: https://mail.dea.com/Exchange/ *(make sure you end with a slash) i.e. https://mail.dea.com/exchange/*

Public folder url: https://mail.dea.com/public/ *(make sure you end with a slash) i.e. https://mail.dea.com/public/*

□ Use Forms Based Authentication (FBA)

Forms based authentication url:

How should we locate the user's portion of their OWA path

Build Using: LDAP Property

Active Directory Mailbox Property Format: {0} *i.e. {0} or {0}_{1}*

Active Directory Mailbox Properties: mailnickname *i.e. Mailnickname or givenname|sn*

Attendee lookup Info

LDAP authentication method: Secure

Path to LDAP: LDAP://dea.com *(Probably need to capitalize LDAP) i.e. LDAP://yourcompany.com*

LDAP query to find attendees (including currently logged in user):

```
(&(|(mailnickname={0}*)(givenname={0}*)(sn={0}*)(mail={0}
*))(|(&(objectCategory=person)(objectClass=user)(|
(homeMDB=*)(msExchHomeServerName=*)))(&
(objectCategory=person)(objectClass=contact))
(objectCategory=group)))
```

LDAP query to find attendees when there is a space in the search string:

```
(&(|(mailnickname={0}*)(givenname={0}*)(sn={0}*)(mail={0}
*))(|(&(objectCategory=person)(objectClass=user)(!
(homeMDB=*))(!(msExchHomeServerName=*)))(&
(objectCategory=person)(objectClass=user)(|(homeMDB=*)
(msExchHomeServerName=*)))(&(objectCategory=person)
```

10. Enter your **Outlook Web Access (OWA) UR**L (example – https://mail.YourCompany.com/exchange/)
11. Enter your **Public Folder URL** (example – https://mail.YourCompany.com/public/)
12. Check the **Use Forms Based Authentication (FBA**) checkbox if FBA is enabled in your environment. Specify the **Forms based authentication url**.
13. Enter your **Path to LDAP** (example – LDAP://YourCompany.com)

    Note: The default settings within the *How should we locate the user's portion of their OWA path* area are appropriate for the majority of installations. For more information about these settings, please see the Optional Settings section.

14. Click **Save**.
15. Go to the **Test Settings** tab.
16. In the **Test Email** field, enter a fully qualified email address (example - John.Smith@YourCompany.com).

    Note: When testing PAM, the email account that is being used (either on the Test Settings tab or in the Testing PAM section below) MUST exist in the Exchange environment being tested. If you are testing PAM in a development environment please verify that a mailbox for the email being used exists in that domain/environment.

17. Click **Test Configuration**. If any errors are encountered, please verify your configuration. Otherwise, your PAM configuration is complete. Please go to the EMS Configuration section below.

Configuring EMS

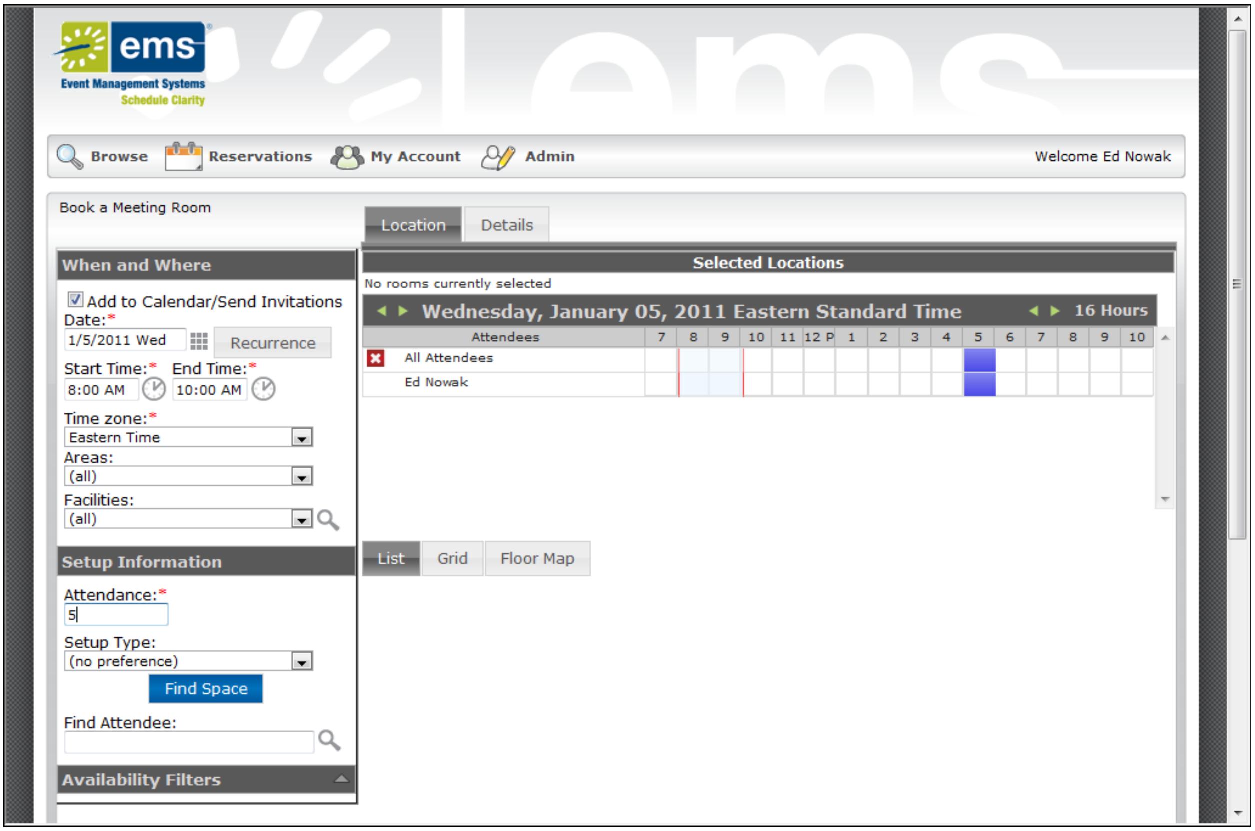
1. Launch your EMS desktop client application. Log in as a user with System Administrator-level access.
2. Go to ***System Administration > Settings > Parameters > EMS*** and locate the parameter – "PAM – *PAM Web Service URL*". Enter the URL of your PAM Web Service.

   http://[ServerName]/PAMWebService/Service.asmx (replace [ServerName] with the name of your web server)

Testing PAM

In order to test your PAM configuration, you will need to log into Virtual EMS with a web user account (configured with the web user's primary email address) belonging to a Web Process Template (within the EMS client application) that has the **Allow Invitations** option checked.

1. Log into Virtual EMS. Go to ***Reservations > Room Request***.



☑ Add to Calendar/Send Invitations

Date:* 1/5/2011 Wed

Start Time:* 8:00 AM End Time:* 10:00 AM

Time zone:* Eastern Time

Areas: (all)

Facilities: (all)

Attendance:* 5

Setup Type: (no preference)

Find Attendee:

No rooms currently selected

Wednesday, January 05, 2011 Eastern Standard Time — 16 Hours

Attendees	7	8	9	10	11	12 P	1	2	3	4	5	6	7	8	9	10
All Attendees											■					
Ed Nowak											■					

2. Enter '*When and Where*' criteria and hit **Find Space**. Select a room.
3. Select the **Add to Calendar/Send Invitations** checkbox. If this option is not available, please verify (within the EMS client application) that your web user account belongs to a Web Process Template that has the **Allow Invitations** option checked.
4. Add an attendee by typing an attendee name in the **Find Attendee** textbox and hitting the magnifying glass icon.
5. Complete necessary information on the **Details** tab and click **Submit Reservation**.
6. Verify that an appointment was added to your Outlook Calendar and that your attendee received an invitation.

Optional Settings

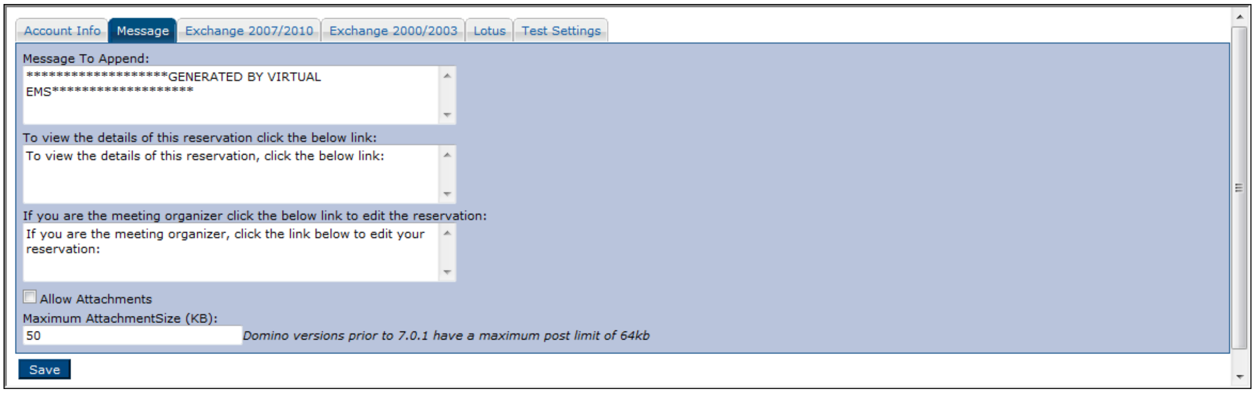
Account Info Tab

Note: See screenshot in Required Settings section.

- **Additional Columns to Display**
  Pipe-delimited list of columns that are displayed when searching for an attendee. DisplayName (e.g. Mike Wimett) and Email are displayed by default.

- **Directory Service Properties for data**
  Pipe-delimited list of LDAP properties that are returned when searching for an attendee.

Message Tab



Message To Append:
*******************GENERATED BY VIRTUAL EMS*******************

To view the details of this reservation click the below link:
To view the details of this reservation, click the below link:

If you are the meeting organizer click the below link to edit the reservation:
If you are the meeting organizer, click the link below to edit your reservation:

□ Allow Attachments

Maximum AttachmentSize (KB):
50 *Domino versions prior to 7.0.1 have a maximum post limit of 64kb*

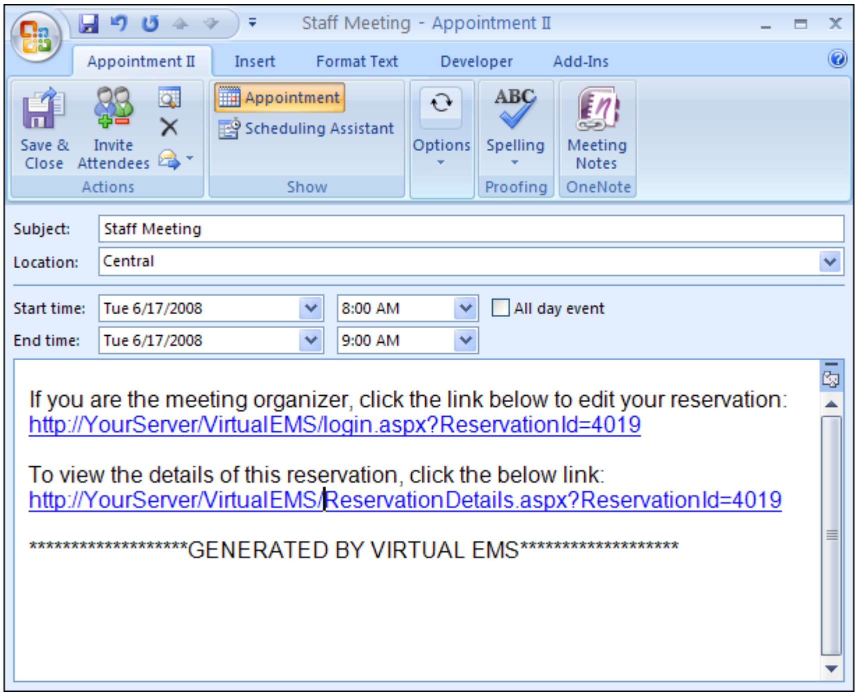
- **Message To Append**
  Message appended to the bottom of the appointment body. This message is seen by all users.

- **To view the details of this reservation click the below link**
  Message added to the appointment body, above a link that takes a user to a view-only Virtual EMS page for the appointment. This message is seen by all users.

- **If you are the meeting organizer click the below link to edit the reservation**
  Message added to the appointment body, above a link that takes the meeting organizer to the Virtual EMS Reservation Summary page for that reservation. This message is seen by all users, but only the meeting organizer can access the Reservation Summary page to make changes.

- **Allow Attachments**
  Allows users to add attachments within Virtual EMS when making an appointment.

- **Maximum AttachmentSize**
  If attachments are allowed, sets the maximum file size allowed for an attachment.



Subject: Staff Meeting

Location: Central

Start time: Tue 6/17/2008 8:00 AM □ All day event

End time: Tue 6/17/2008 9:00 AM

If you are the meeting organizer, click the link below to edit your reservation:
http://YourServer/VirtualEMS/login.aspx?ReservationId=4019

To view the details of this reservation, click the below link:
http://YourServer/VirtualEMS/ReservationDetails.aspx?ReservationId=4019

*******************GENERATED BY VIRTUAL EMS*******************

Exchange 2000/2003 Tab

Note: See screenshot in Required Settings section.

- **Build Using**
  Determines how a Virtual EMS user’s OWA calendar path is determined.

- **Active Directory Mailbox Property Format**
  If the current Microsoft Active Directory structure is set to use anything other than mailnickname (e.g., givenname\surname), the correct entries need to be made in this field and the Active Directory Mailbox Properties field. If you have questions, or if Active Directory has a different structure than the one given here, contact Customer Support.

- **Active Directory Mailbox Properties**
  If the current Microsoft Active Directory structure is set to use anything other than mailnickname, enter *givenname*|*sn*.

- **LDAP authentication method**
  Determines the LDAP authentication method when looking-up an attendee.

- **LDAP query to find attendees + LDAP query to find attendees when there is a space in the search string**
  These two LDAP queries are only to be edited when special circumstances arise with unique configurations of Microsoft Exchange and LDAP. If you choose to edit any of the queries, you should do so ***only if you are well-versed in developing and editing LDAP queries***. Before you begin editing a query, be sure to make a copy of the original query text.

Additional Information

Use Application Pool Identity for Service Account

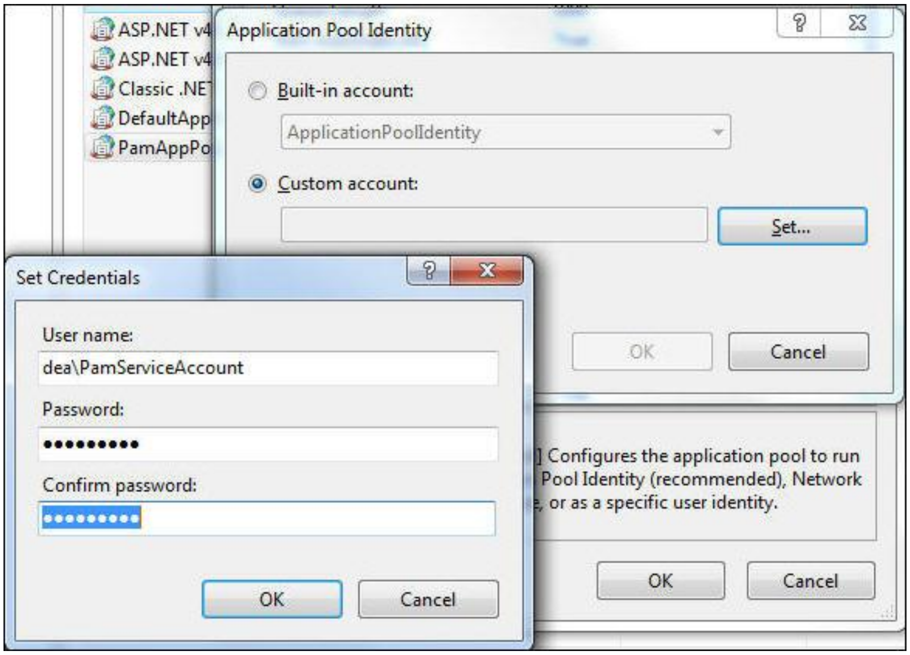
Rather than inputting the PAM Account credentials on the PAMConfig.aspx page, credentials can be maintained at the Application Pool level. This allows your organization to maintain absolute control – **only** IIS applications running in the newly created application pool can run as the PAM Account.

This functionality requires the following:

- Microsoft Exchange 2007 (SP1) or Exchange 2010. Note, Exchange 2003 or Mixed Mode Exchange 2003 + 2007/2010 environments **do not** support this functionality.
- Microsoft Exchange Impersonation Account (PAM Account). This account **must** be using Impersonation, not full access to the mailbox store.

To configure the Application Pool

1. Open IIS Manager
2. Open the *Application Pools* panel
3. Click *Add Application Pool…*
4. The *Add Application Pool* window opens. Enter a unique name and ensure .NET Framework v2.0 is selected. Managed pipeline mode should be *Integrated*. Click OK
5. Find the Application Pool you just created. Right-click it and select *Advanced Settings*
6. The third section in the list is *Process Model*. Highlight *Identity* and then click the ... button to configure.
7. Choose *Custom Account* and then click Set. Enter the username and password for your PAM Account. Confirm the password and click OK on any remaining dialogs (see screenshot below)



User name: dea\PamServiceAccount

Password: •••••••••

Confirm password: •••••••••

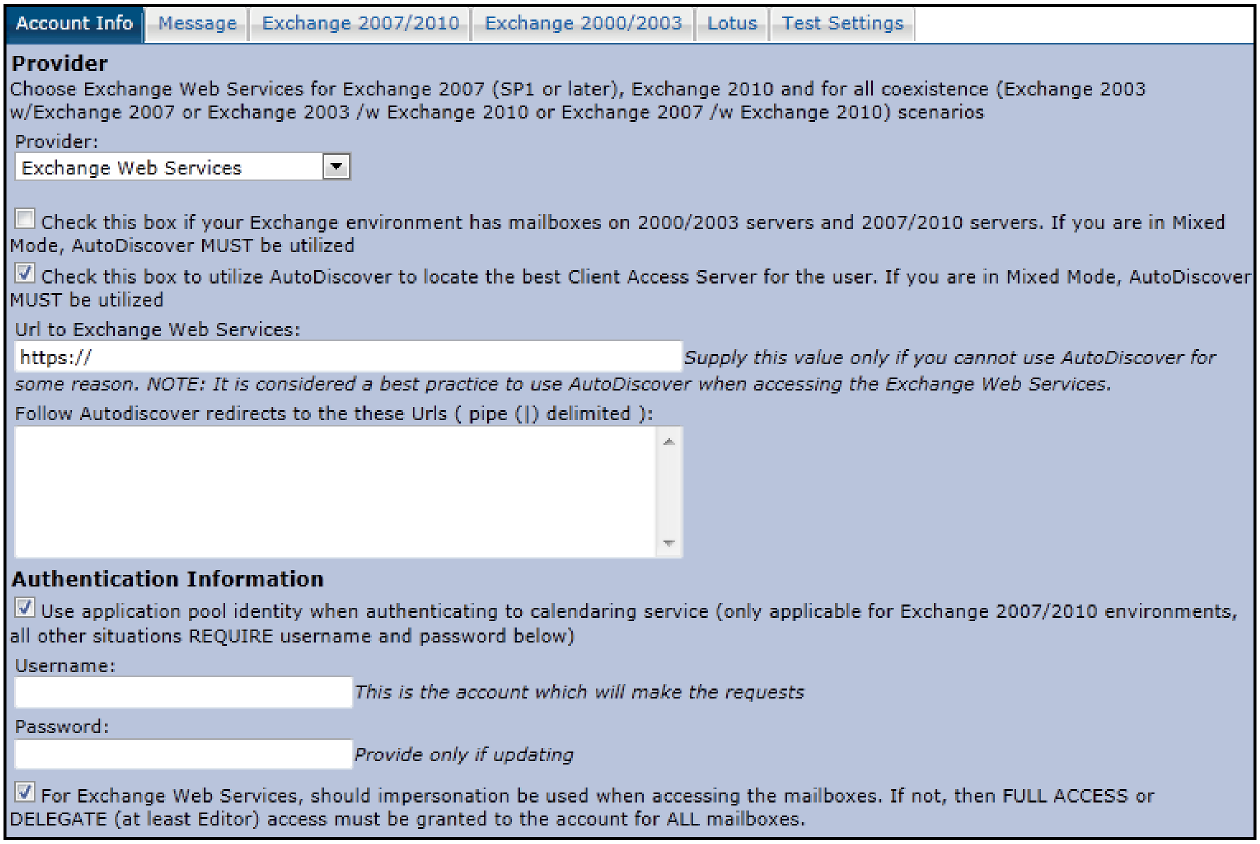
8. Within IIS Manager, navigate to the Virtual Directory containing the PAM Web Service. This is under the Default Web Site by default, but may be installed to a different web site.
9. With the PamWebService Virtual Directory highlighted in the left pane, select *Basic Settings…* under Actions in the right pane.
10. Click the *Select…* button and then choose your newly created application pool from the list.
11. Click OK on all remaining dialogs.
12. You may need to restart IIS for the change to take effect.

To configure Plan-a-Meeting to use the Application Pool account

1. Navigate to the PAM configuration area by opening a browser and entering the following:

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

2. From the *Account Info* tab, find the *Authentication Information* section, check the box for *"Use application pool identity when authenticating to calendaring service"* (see screenshot below)



Provider

Choose Exchange Web Services for Exchange 2007 (SP1 or later), Exchange 2010 and for all coexistence (Exchange 2003 w/Exchange 2007 or Exchange 2003 /w Exchange 2010 or Exchange 2007 /w Exchange 2010) scenarios

Provider: Exchange Web Services

□ Check this box if your Exchange environment has mailboxes on 2000/2003 servers and 2007/2010 servers. If you are in Mixed Mode, AutoDiscover MUST be utilized

☑ Check this box to utilize AutoDiscover to locate the best Client Access Server for the user. If you are in Mixed Mode, AutoDiscover MUST be utilized

Url to Exchange Web Services: https:// *Supply this value only if you cannot use AutoDiscover for some reason. NOTE: It is considered a best practice to use AutoDiscover when accessing the Exchange Web Services.*

Follow Autodiscover redirects to the these Urls (pipe (|) delimited):

Authentication Information

☑ Use application pool identity when authenticating to calendaring service (only applicable for Exchange 2007/2010 environments, all other situations REQUIRE username and password below)

Username: *This is the account which will make the requests*

Password: *Provide only if updating*

☑ For Exchange Web Services, should impersonation be used when accessing the mailboxes. If not, then FULL ACCESS or DELEGATE (at least Editor) access must be granted to the account for ALL mailboxes.

3. With this option enabled, you can leave blank the *Username* and *Password* fields in the Authentication Information section.
4. Click the *Save* button at the bottom of the page.