Workspace ONE UEM Certificate Authentication for EAS with NDES-MSCEP

VMware Workspace ONE UEM 1902

vmware®

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

If you have comments about this documentation, submit your feedback to

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Workspace ONE UEM Certificate Authentication for EAS with NDES-MSCEP

1

This documentation explains the configurations required for the Microsoft Exchange Client Access Server (CAS) and Workspace ONE UEM to allow a device to connect to Microsoft Exchange ActiveSync (EAS) using a certificate for authentication.

Prerequisites for EAS with NDES-MSCEP

The following tasks must be completed before proceeding with the steps outlined in this documentation.

- A certificate authority server must be set up and configured as described in Setting up a Microsoft CA for NDES/SCEP/MSCEP.The CA must be an Enterprise CA as opposed to a Stand Alone CA (Stand Alone does not allow for the configuration and customization of templates).
    - A Network Device Enrollment Service, also referred to as MSCEP server setup. NDES is only available in the Enterprise version of Microsoft Server 2008 and 2008 R2.
- Microsoft Exchange with ActiveSync enabled.
- Internet Information Services (IIS) on the EAS server must have the option "Client Certificate Mapping Authentication" installed.

Install, Set Up, Configure Certificate

2

This section provides instructions to configure the certificate authority (CA) of your choice to work with the Workspace ONE ™ UEM console.

Take the following steps and procedures to integrate the certificate.

This chapter includes the following topics:

- Step 1: Set Up a Trust between Active Directory and the Certificate Authority, EAS with NDES-MSCEP
- Step 2: Set Permissions on Exchange Server
- Step 3: Configuring Certificate Authority And Certificate Template In Workspace ONE UEM, EAS with NDES-MSCEP
- Step 4: Create Profile for Exchange ActiveSync, EAS with NDES-MSCEP

Step 1: Set Up a Trust between Active Directory and the Certificate Authority, EAS with NDES-MSCEP

In order for Microsoft Exchange ActiveSync to authenticate a user from a certificate, it must first trust the source of the certificate.
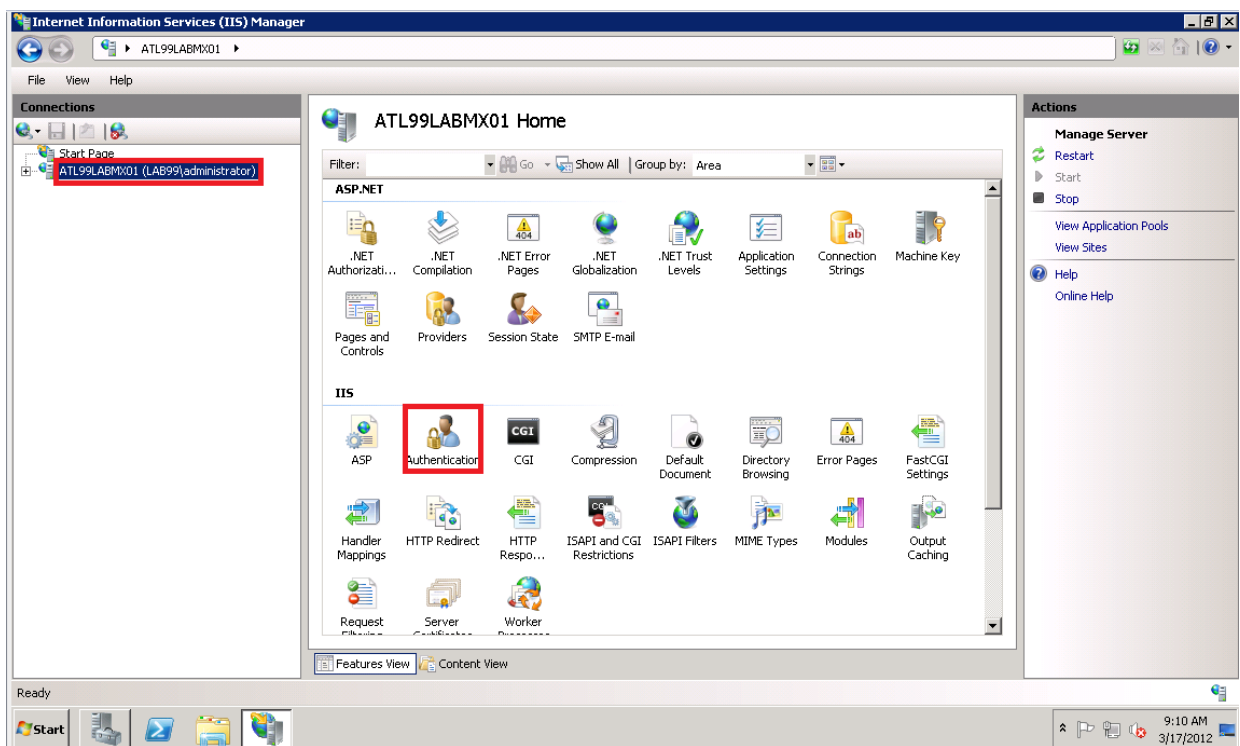
1   On the Certificate Authority server, select **Start > Run**.

2   Type MMC in the dialog box and press **Enter** to launch the Microsoft Management Console (MMC).

3   Click **File > Add/Remove Snap-in…** from the MMC main menu.

4   Select **Enterprise PKI** from the list of Available snap-ins and then select **Add**.

5   Click **OK**.

6   Right-click **Enterprise PKI** and select **Manage AD Containers**.

7   Select the **NT AuthCertificates** tab and verify the Certificate Authority is listed. If not, select **Add** to add the Certificate Authority to the group.

8   Click **OK**.

Step 2: Set Permissions on Exchange Server

In order for devices to authenticate with Microsoft Exchange ActiveSync, you must configure several changes on the Exchange Server.

Certificate Authentication

1   On the Exchange server, select **Start > Run**.

2   Type `inetmgr` in the dialog box to run **Internet Information Services (IIS)**.

3   Select the server in the **Connections** pane.

4   Under IIS, double-click the **Authentication** icon.

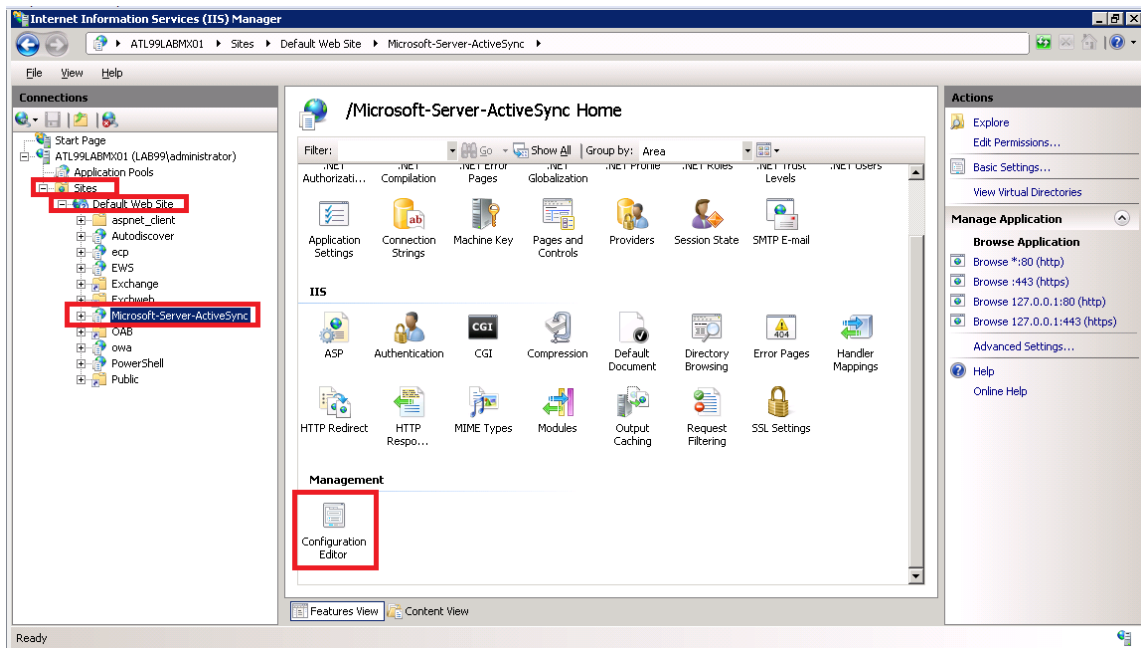5   Select **Active Directory Client Certificate Authentication** and then select **Enable**.

Configuration Editor

1   Select **+** to expand **Site** and then **Default website** to display all available configuration editors.

   a   If you are using MS Server 2008 R2 or later, the **Configuration Editor** icon appears; Select **Microsoft-Server-ActiveSync** and double-click on the **Configuration Editor** icon. Skip steps **1b** & **1c**, and go directly to step 2.

   b   If you are using Exchange servers older than 2008 R2, be familiar with the use of **appcmd.exe** and run it from the command prompt.

    c   Open a command prompt by selecting **Start > Run**. Type `cmd` in the dialog box and select **OK**. In the command prompt, type the following command:
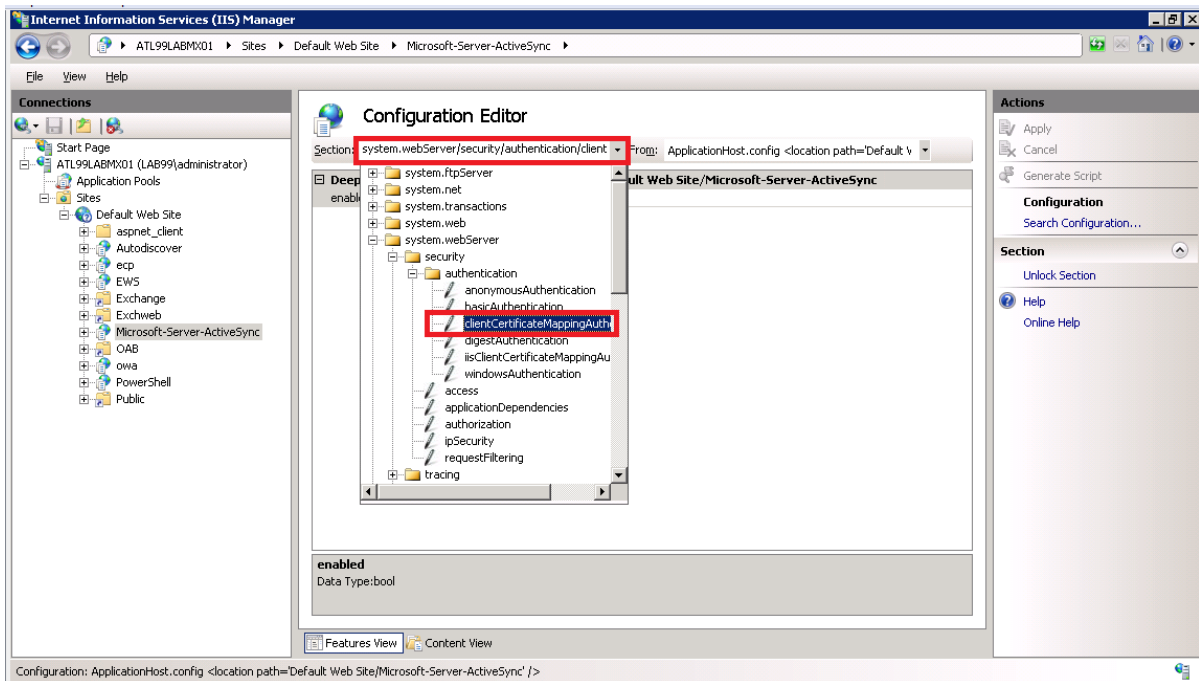
```
appcmd.exe set config "Microsoft-Server-ActiveSync" -
section:system.webServer/security/authentication/clientCertificateMappingAuth
entication /enabled:"True" /commit:apphost
```

If you performed this step, then skip the remaining steps and advance to Setting up Secure Socket Layer (SSL).

2   Navigate to **system.webserver/security/authentication** in the Section drop-down menu.

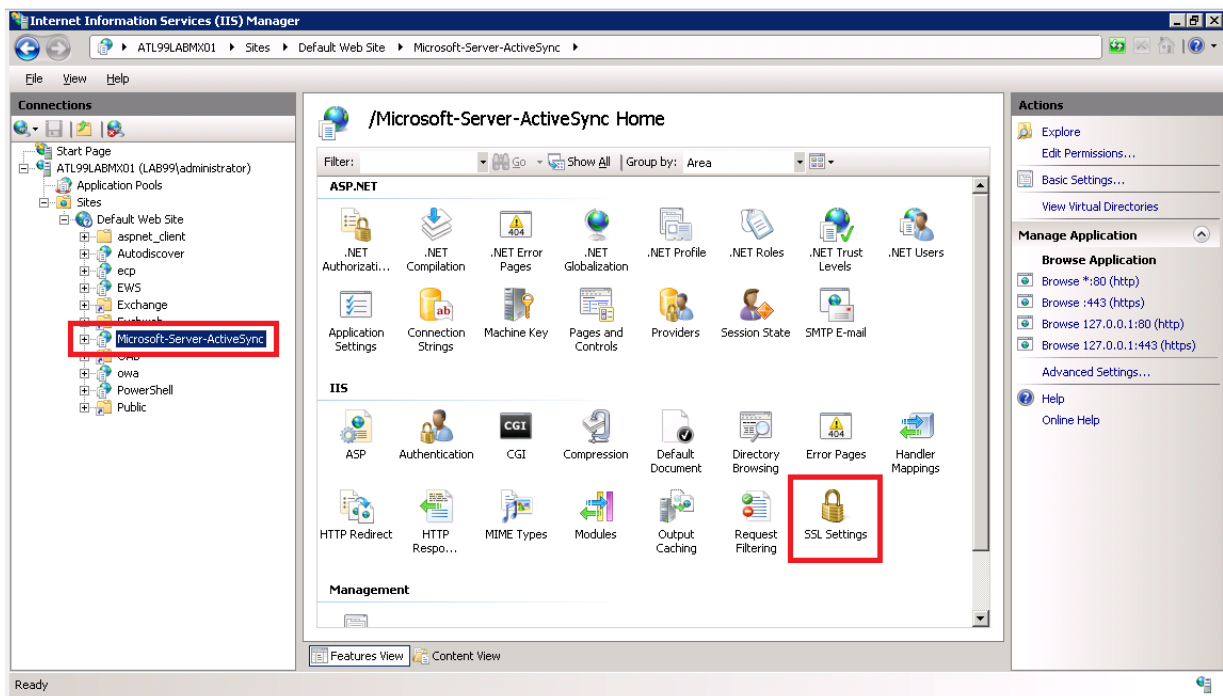3   Select **clientCertificateMappingAuthentication**.

4   Select **True** from the drop-down menu on the Enabled option.

Set Up Secure Socket Layer

If only certificate authentication is being used, then you must configure Secure Socket Layer (SSL).

1   Select **Microsoft-Server-ActiveSync**, and then double-click the **SSL Settings** icon.

2 Select **Accept** if other types of authentication are allowed. If only certificate authentication is allowed, then select the **Require SSL** check box and then select **Required**.

Adjust uploadReadAheadSize Memory Size

Since certificate-based authentication uses a larger amount of data during the authentication process, you must increase the value of the **uploadReadAheadSize** from 48 KB to 10 MB to account for the increased amount of data. Specifically, The following steps guide you through the configuration:

1 Open a command prompt by selecting **Start > Run**.

2 Type cmd in the dialog box and select OK.

3 Enter the following commands:

```
C:\Windows\System32\inetsrv\appcmd.exe set config –
section:system.webServer/serverRuntime /uploadReadAheadSize:"10485760" /commit:apphost
```

```
C:\Windows\System32\inetsrv\appcmd.exe set config "Default Website" –
section:system.webServer/serverRuntime /uploadReadAheadSize:"10485760" /commit:apphost
```

If the name of the site has been changed in IIS, then replace `Default Website` with the new name in the second command.

4 Perform an IIS reset by entering the following command:

```
iisreset
```

Step 3: Configuring Certificate Authority And Certificate Template In Workspace ONE UEM, EAS with NDES-MSCEP

In order for Workspace ONE UEM to retrieve a certificate from a certificate authority, you must correctly configure the Workspace ONE UEM console to use the certificate. There are two steps to this process.

- Configure the certificate authority.

- Configure the certificate template.

1 Open the Workspace ONE UEM console.

2 Login as a user with Workspace ONE UEM Administrator privileges or higher.

3 Navigate to **Devices > Certificates > Certificate Authorities**.

4 Click **Add**.

5 Select from the **Generic SCEP** from the Authority Type drop-down menu prior to completing any other configuration settings for the certificate authority.

6   Enter the following details about the CA in the remaining fields:

- Enter the actual certificate authority Name in the **Certificate Authority** field. This is the name of the CA to which the NDES/SCEP/MSCEP endpoint is connected. This can be found by launching the **Certification Authority** application on the CA server.

- Enter a brief **Description** for the new CA.

- Enter the URL of the CA server in the **SCEP URL** field.

- Select the **Challenge Type** radio button that reflects whether or not a challenge phrase is required for authentication. For additional authentication, choose **Static** or **No Challenge**.

  - If you select **Static,** enter an authentication phrase consisting of a key or password used to authenticate the device with the certificate enrollment URL.

7   Click **Test Connection**. If you select Save prior to **Test Connection**, a "Test is unsuccessful" error displays.

8   Click **Save**.

9   Select the **Request Templates** tab

10   Click **Add** to add a new certificate template.

11   Complete the certificate template information:

- Enter a name for the new **Request Template**.

- Enter a brief **Description** for the new certificate template.

- Select the certificate authority that was just created from the **Certificate Authority** drop-down menu.

- Enter the **Subject Name** or Distinguished Name (DN) for the template. The text entered in this field is the "Subject" of the certificate, which can be used by the network administrator to determine who or what device received the certificate.

  A typical entry in this field is "CN=WorkspaceONEUEM.{EnrollmentUser}" or "CN={DeviceUid}" where the {} fields are Workspace ONE UEM lookup values.

- Select the private key length from the **Private Key Length** drop-down box.:

  This is typically 2048 and should match the setting on the certificate template that is being used by NDES/SCEP/MSCEP.

- Select the **Private Key Type** using the applicable checkbox.

  This should match the setting on the certificate template that is being used by NDES/SCEP/MSCEP.

- Click **Add** to the right of **SAN Type** to include one or more Subject Alternate Names with the template. This is used for additional unique certificate identification. In most cases, this needs to match the certificate template on the server. Use the drop-down menu to select the SAN Type and enter the subject alternate name in the corresponding data entry field. Each field supports lookup values.

- Select the **Automatic Certificate Renewal** checkbox to have certificates using this template automatically renewed prior to their expiration date. If enabled, specify the Auto Renewal Period in days.

- Select the **Enable Certificate Revocation** checkbox to have certificates automatically revoked when applicable devices are unenrolled or deleted, or if the applicable profile is removed.

- Select the **Publish Private Key** checkbox to publish the private key to the specified web service endpoint (Directory Services or custom web service)

12 Click **Save**.

Step 4: Create Profile for Exchange ActiveSync, EAS with NDES-MSCEP

The final step in setting up the Exchange Active Sync Certificate Authentication is creating and deploying the Workspace ONE UEM profile that pushes the Exchange Server settings to the device. This profile contains the information necessary for the device to connect to Exchange, as well as the certificate that the device uses to authenticate.

1 Navigate to **Devices > Profiles > List View**.

2 Click **Add**.

3 Click the applicable device platform to launch the **Add a New Profile** dialog.

4 Configure the **General** settings for the profile. The General settings determine how the profile is deployed and who receives it as well as other overall settings.

5 Select **Credentials** from the profile options at left and then select **Configure**.

6 Select **Define Certificate Authority** from the Credential Source drop-down menu.

7 Select the certificate authority you created previously from the **Certificate Authority** drop-down menu.

8 Select the certificate template you created previously from the **Certificate Template** drop-down menu.

9 Select **Exchange ActiveSync** from the profile options at left and then select **Configure**.

You must configure the Credentials payload settings before the Exchange ActiveSync payload settings.

10 Configure the **Exchange ActiveSync** settings:

- Enter an account name in the **Account Name** field. This is the name that displays on the device to indicate which email account is active so it should be accurately descriptive.

- Enter the Exchange ActiveSync host in the **Exchange Active Sync Host** data entry field. This is the actual endpoint of the mail server.

  Do not include â€œhttp://â€, â€œhttps://â€ at the beginning or â€œ/Microsoft-server-activesyncâ€ at the end.

- Ensure the **Use SSL** checkbox is selected. Authentication using certificates fails over a non-SSL connection.

- Deselect the **Use S/MIME** checkbox if enabled by default.

- The **Domain** data entry field should contain the email domain for the user account.

- The **Username** data entry field should contain the email address of the user when on the device.

- The **Email Address** text box should contain the email address of the user when on the device

  Domain, Username, and Email Address can be obtained using Lookup Values which will retrieve the text stored in the applicable field of the User Profile.

- Select the credential you created previously from the **Payload Certificate** drop-down menu.

11 Click **Save** or select **Save and Publish** to publish this profile to a device.

Testing and Troubleshooting, EAS with NDES-MSCEP 3

You can confirm that the certificate is operational by pushing a profile to the device and testing whether or not the device is able to connect and sync to the configured Exchange ActiveSync endpoint. If the device does not connect and shows a message indicating the certificate cannot be authenticated or the account cannot connect to Exchange ActiveSync, then there is a problem in the configuration.

Ensure a certificate is being issued by the certificate authority to the device by checking the following information:

1   Launch the certification authority application on the certificate authority server and browse to the issued certificates section.

2   Locate the last certificate issued and verify it shows a subject matching the subject created when the certificate was generated in the Workspace ONE UEM console.

    If there is no certificate, then there is an issue with the certificate authority, client access server (e.g., ADCS), or the Workspace ONE UEM connection to client access server.

3   Ensure the permissions of the client access server (e.g., ADCS) Admin Account is applied correctly to the certificate authority and the certificate template.

4   Ensure the account information is entered correctly in the Workspace ONE UEMconfiguration.

If the certificate is being issued, ensure that it is in the profile and on the device:

1   Navigate to **Devices > Profiles > List View**.

2   Click to the right of the applicable Exchange ActiveSync profile to launch the Actions menu and select View XML.

3   On the device, access the list of installed profiles.

4   View details for the applicable profile and ensure the certificate is present.

5   Confirm that the certificate contains the **Subject Alternative Name** (or SAN) section and within that section there is an **Email** and **Principal** name with the appropriate data. If this section is not in the certificate, then either the template is incorrect or the certificate authority has not been configured to accept SAN. Refer to the section on configuring the certificate authority.

6   Confirm the certificate contains the **Client Authentication** in the **Enhanced Key Usage** section. If not present, then the template is not configured correctly.

If the certificate is on the device and contains the correct information, then the problem is most likely with the security settings on the Exchange ActiveSync server. Confirm the address of the Exchange ActiveSync server is entered correctly in the Workspace ONE UEMprofile and that all security settings have been adjusted to allow certificate authentication on the Exchange ActiveSync server.

A reliable test is to manually configure a single device to connect to the Exchange ActiveSync server using certificate authentication. This should work outside of Workspace ONE UEM and until this works properly, Workspace ONE UEM will not be able to configure a device to connect to Exchange ActiveSync with a certificate.