CISSP - Profesional certificado en seguridad de sistemas de información

Implemente SSL VPN usando el administrador de dispositivos ASA

Introducción

El implemente ssl VPN usando el módulo **del administrador de dispositivos ASA** le proporciona las instrucciones y el hardware de Cisco para desarrollar sus habilidades prácticas en los temas siguientes:

- Implemente un Clientless SSL VPN usando el administrador de dispositivos de Cisco ASA
- Implemente AnyConnect usando el administrador de dispositivos de Cisco ASA

Tiempo de laboratorio: Tomará aproximadamente 1 hora para completar este laboratorio.

> Este módulo refiere a las comunicaciones CISSP y al dominio de seguridad de red. Para comprender completamente este tema, consulte el material de su curso o utilice su motor de búsqueda favorito para investigar este tema con más detalle.

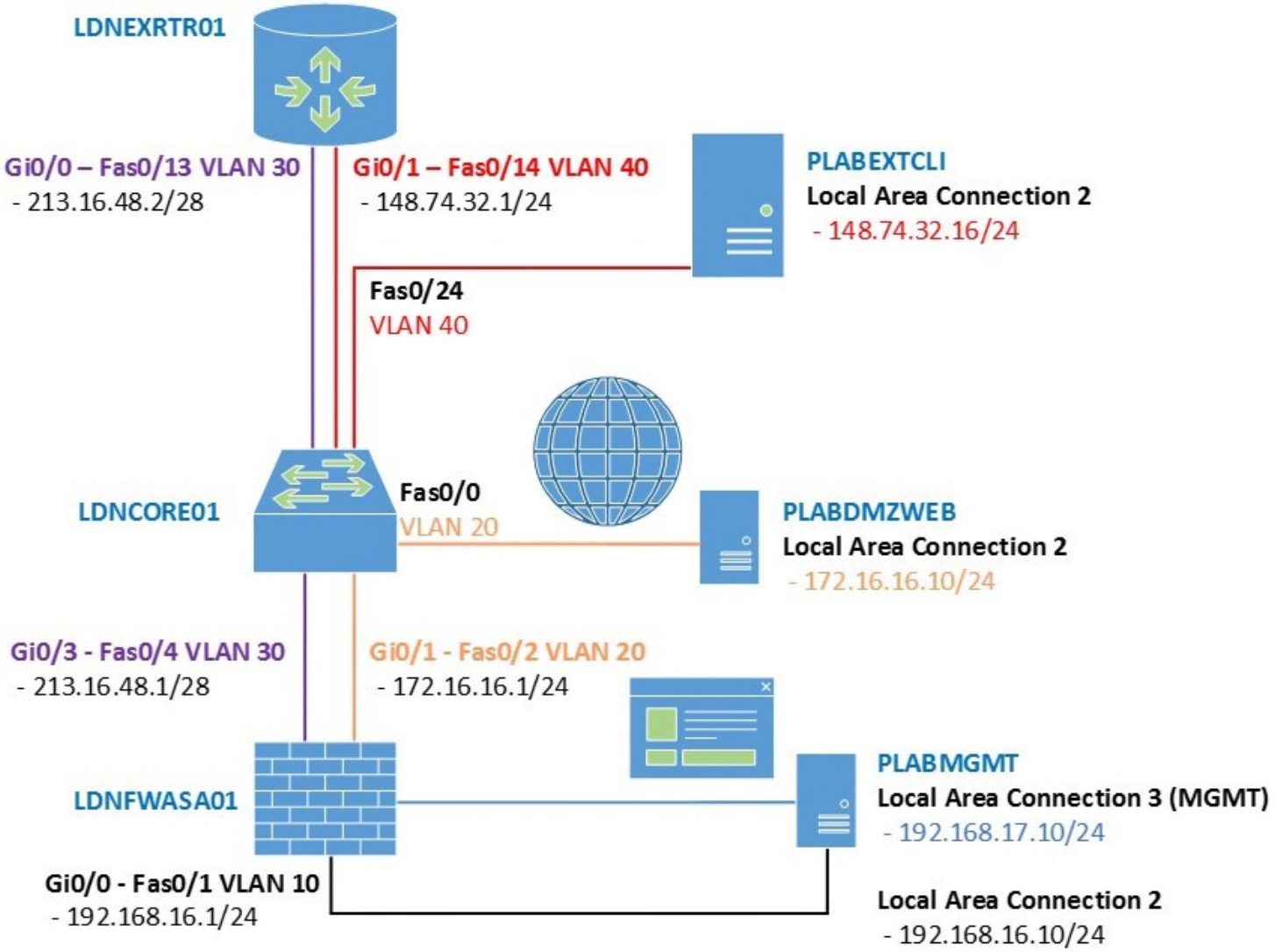
Objetivos del examen

Los siguientes objetivos del examen están cubiertos en este laboratorio:

- Aplicar principios de diseño seguro a la arquitectura de red (por ejemplo, protocolos IP y no IP, segmentación)
- Componentes de red seguros
- Diseñar y establecer canales de comunicación seguros
- Prevenir o mitigar los ataques a la red

Diagrama de laboratorio

Durante la sesión, tendrá acceso a la siguiente configuración de laboratorio. Dependiendo de los ejercicios, puede o no usar todos los dispositivos, pero se muestran aquí en el diseño para obtener una comprensión general de la topología del laboratorio.



Conexión a su laboratorio

En este módulo, estarás trabajando en los siguientes equipos para llevar a cabo los pasos definidos en cada ejercicio.

- LDNFWASA01
- LDNEXTRTR01
- LDNCORE01
- PLABMGMT
- PLABDMZWEB
- PLABEXTCLI

Para empezar, simplemente elija un dispositivo y haga clic **en Encender**. En algunos casos, los dispositivos pueden encenderse automáticamente.

Para obtener más información y soporte técnico, consulte nuestra página de Ayuda y soporte técnico.

Ejercicio 1 - Implemente un Clientless SSL VPN usando el administrador de dispositivos de Cisco ASA

En este ejercicio, usted utilizará el software de Cisco ASDM para crear un Clientless SSL VPN que habilita el acceso remoto para que los usuarios basados en web tengan acceso a

la red corporativa. En este ejemplo en particular, utilizará PLABEXTCLI a VPN al firewall LDNFWASA01 que permite la conectividad con PLABDMZWEB.

Se ha aplicado una configuración base a todos los dispositivos del laboratorio para que pueda centrarse en la configuración de la VPN. La configuración base que se ha aplicado es esa misma configuración que usted construyó en el módulo **implemente el dispositivo de seguridad adaptante de Cisco.**

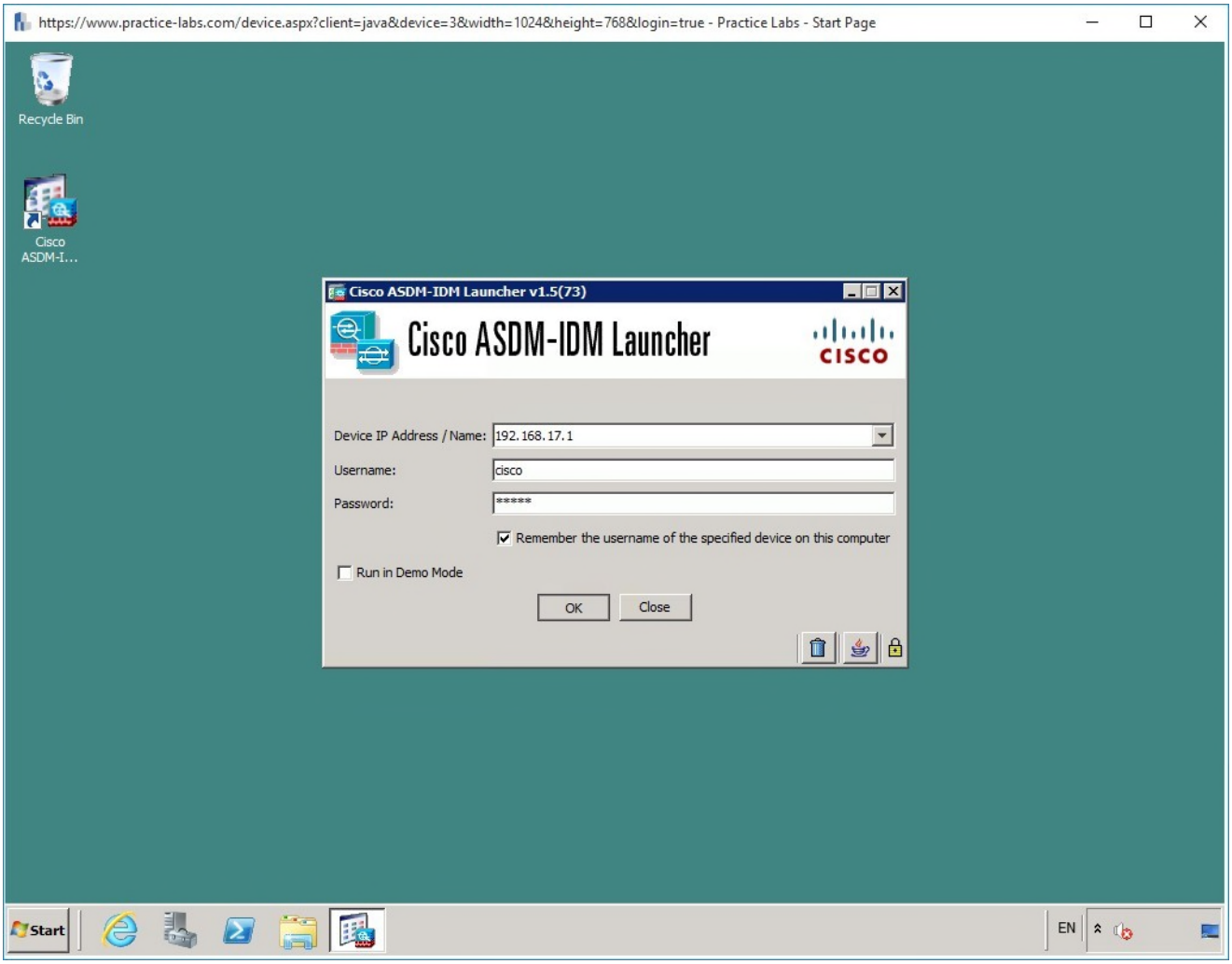
Tarea 1 - Configurar una VPN SSL sin cliente

Para configurar una VPN SSL sin cliente, siga estos pasos:

Paso 1

Asegúrese de que todos los dispositivos estén encendidos en el laboratorio. Una vez que **el PLABMGMT** está para arriba, conecte con el escritorio y abra el software de Cisco ASDM, un icono está situado en el escritorio.

Inicie sesión usando el nombre de usuario **Cisco** y la contraseña **Cisco** que se asegura de que la dirección IP del dispositivo esté fijada a **192.168.17.1:**



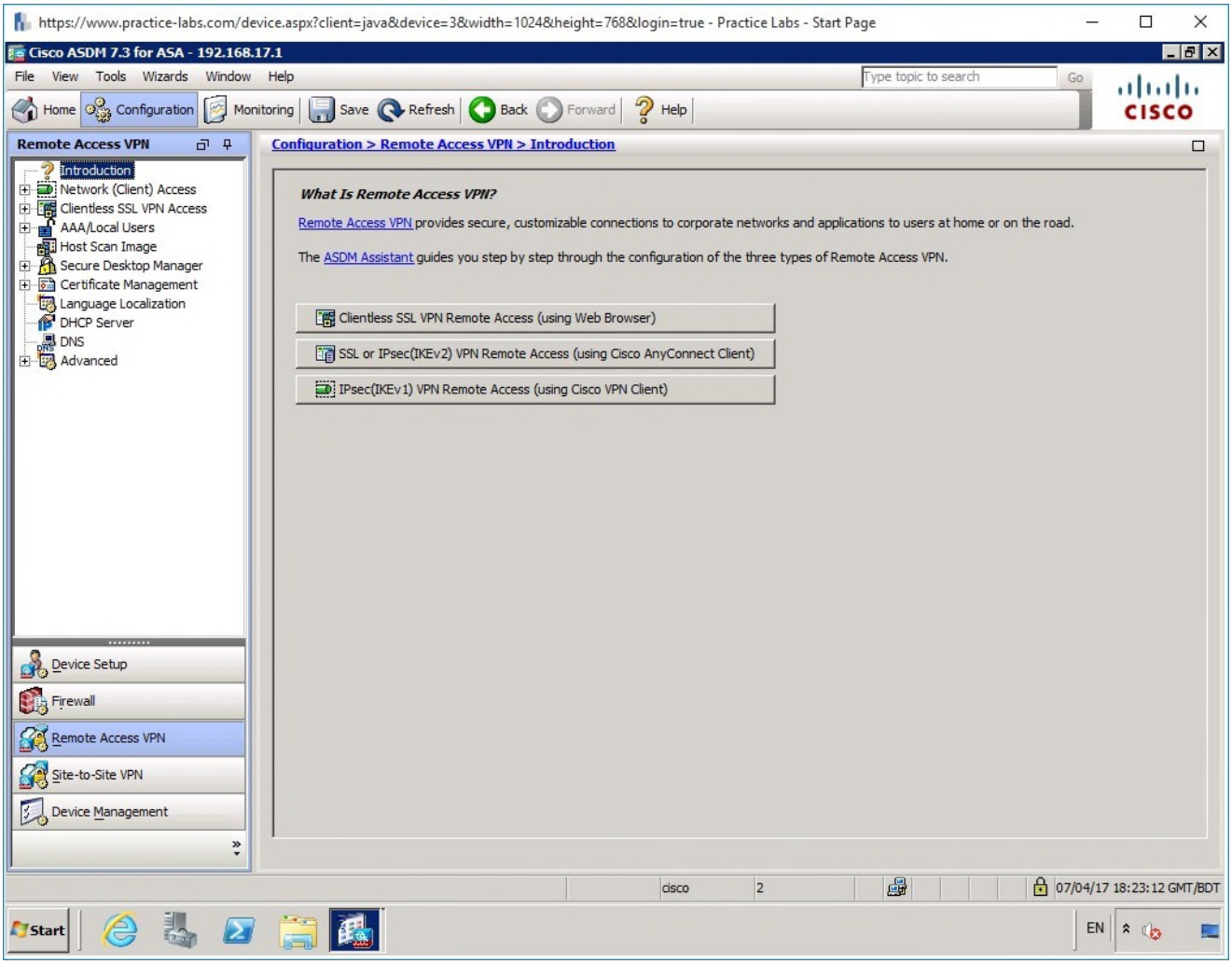
Cuadro 1.1 Captura de pantalla de la ventana inicial del lanzador del Cisco ASDM-IDM: Ésta es la ventana inicial Que el lanzador asdm-IDM de Cisco visualiza una vez que se ejecuta. La dirección IP 192.168.17.1 se ha introducido en el campo "Dirección IP del dispositivo / Nombre". Las credenciales de usuario se introducen en los campos "Nombre de usuario" y "Contraseña".

Presione **la AUTORIZACIÓN** cuando usted ha ingresado en los detalles (asegúrese de que el funcionamiento en el modo de **demostración** sea desmarcado, recuerde que usted está conectando con Cisco verdadero ASA).

Aparecerá una advertencia de seguridad, por lo que haga clic en la casilla de verificación 'Confiar siempre en el contenido de este publicador' y, a continuación, haga clic en **Sí**.

Step 2

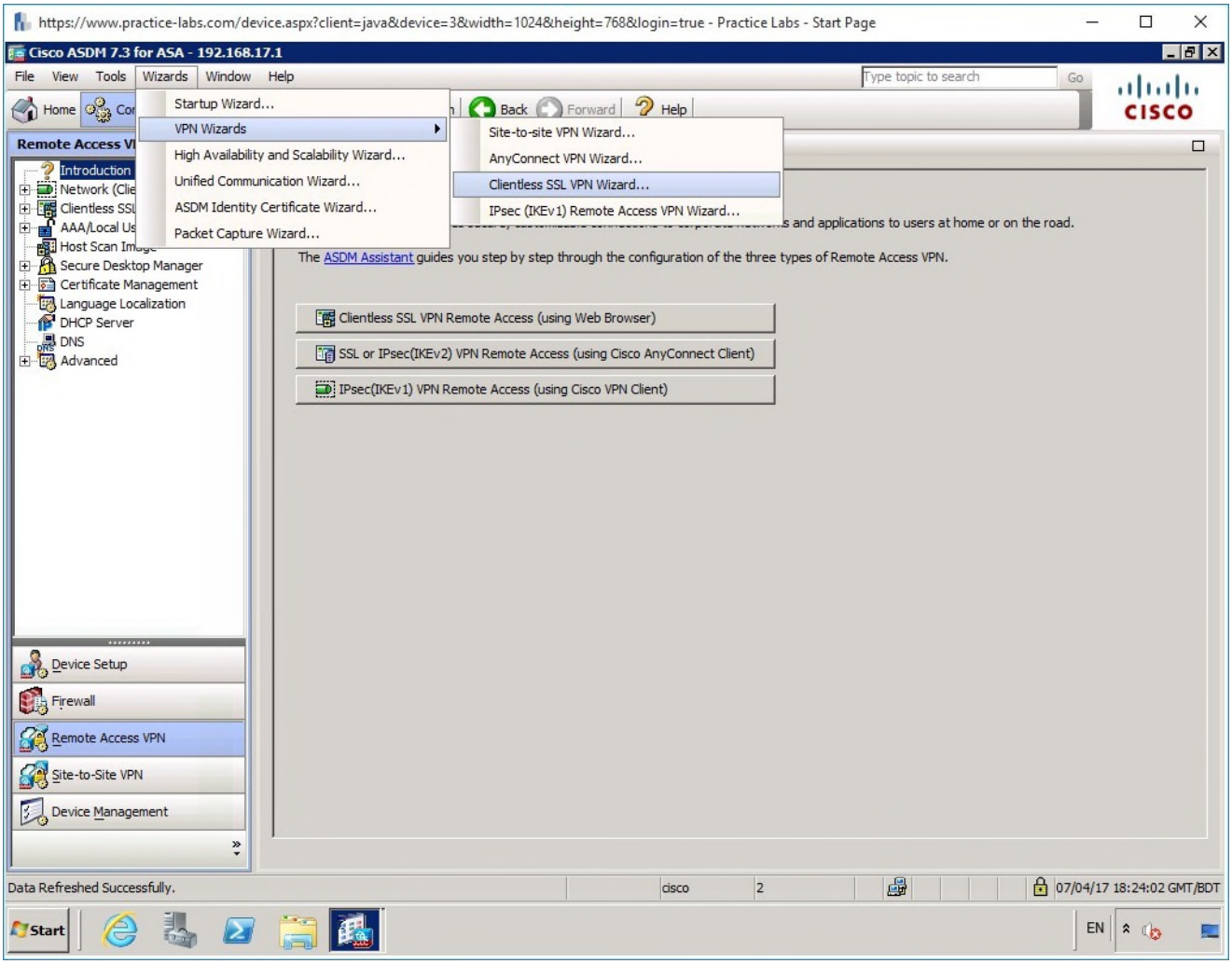
Una vez que el GUI aparece, haga clic el botón **Configuration** Button, después en el panel izquierdo en la parte inferior haga clic el botón **vpn de acceso remoto:**



Cuadro 1.2 Captura de pantalla de la ventana inicial del lanzador del Cisco ASDM-IDM después de la autenticación acertada: Esta pantalla visualiza la conexión al dispositivo en la dirección IP 192.168.17.1. Verá los diferentes tipos de opciones de configuración en esta pantalla.

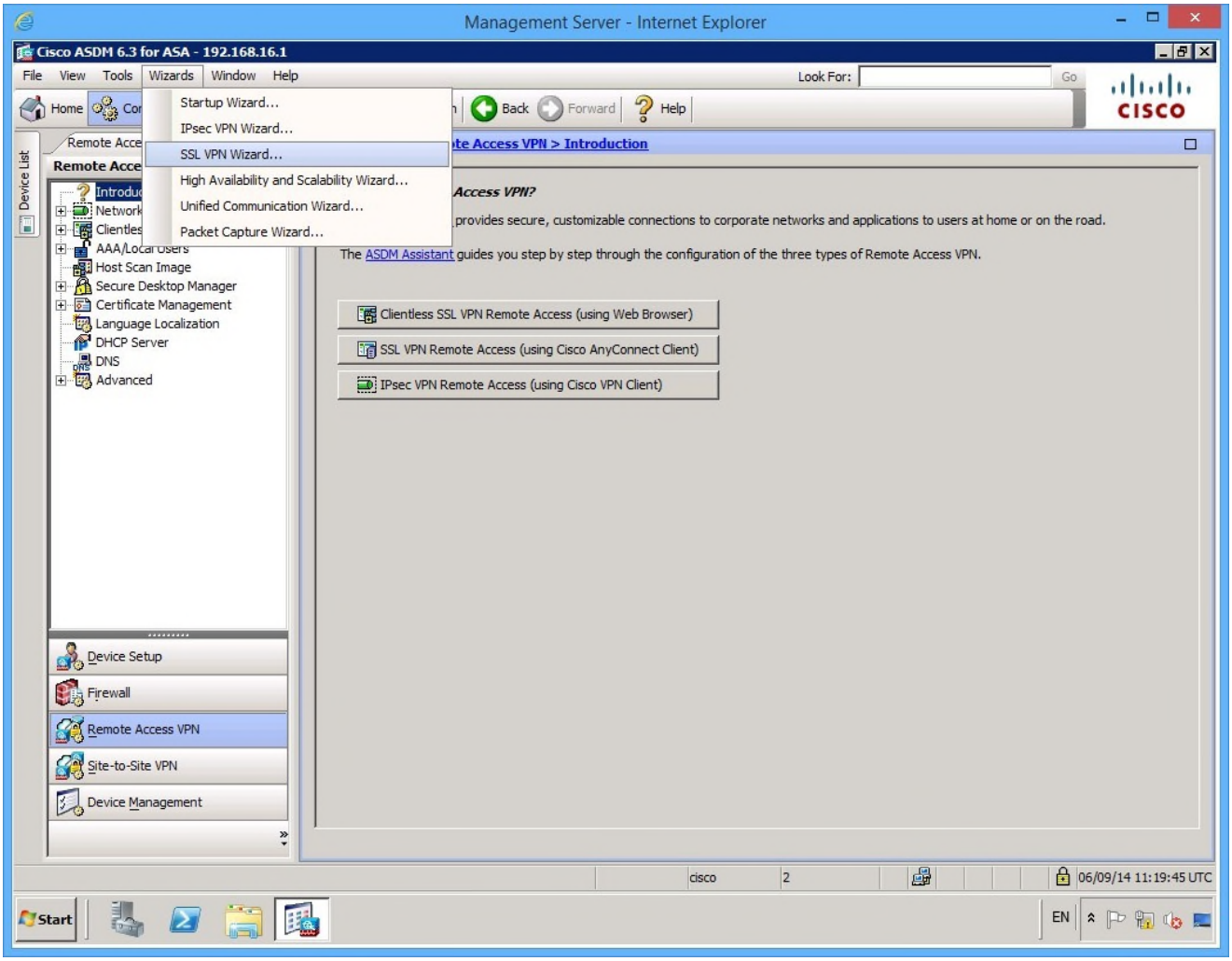
En esta página verá una serie de botones a la derecha, estos simplemente abren un poco de ayuda, no son los asistentes.

En su lugar, necesitamos navegar a través del menú superior **Wizards > VPN Wizards > Clientless SSL VPN Wizard** para iniciar el proceso.



Cuadro 1.3 Captura de pantalla de la ventana de configuración inicial del lanzador del Cisco ASDM-IDM: Después de hacer clic a los asistentes (opciones de menú de los asistentes VPN, usted verá las opciones múltiples de las cuales usted necesita seleccionar al asistente clientless SSL VPN.

Nota: *En más viejas versiones del ASDM, el elemento de menú es levemente diferente, un tiro de pantalla de la más vieja versión se muestra abajo para su referencia.*



Cuadro 1.4 Captura de pantalla de la ventana de configuración inicial del lanzador del Cisco ASDM-IDM: Después de hacer clic a los asistentes, usted necesita seleccionar a los asistentes SSL VPN.

Una vez que inicie el asistente, haga clic en **Siguiente** en esta primera página.

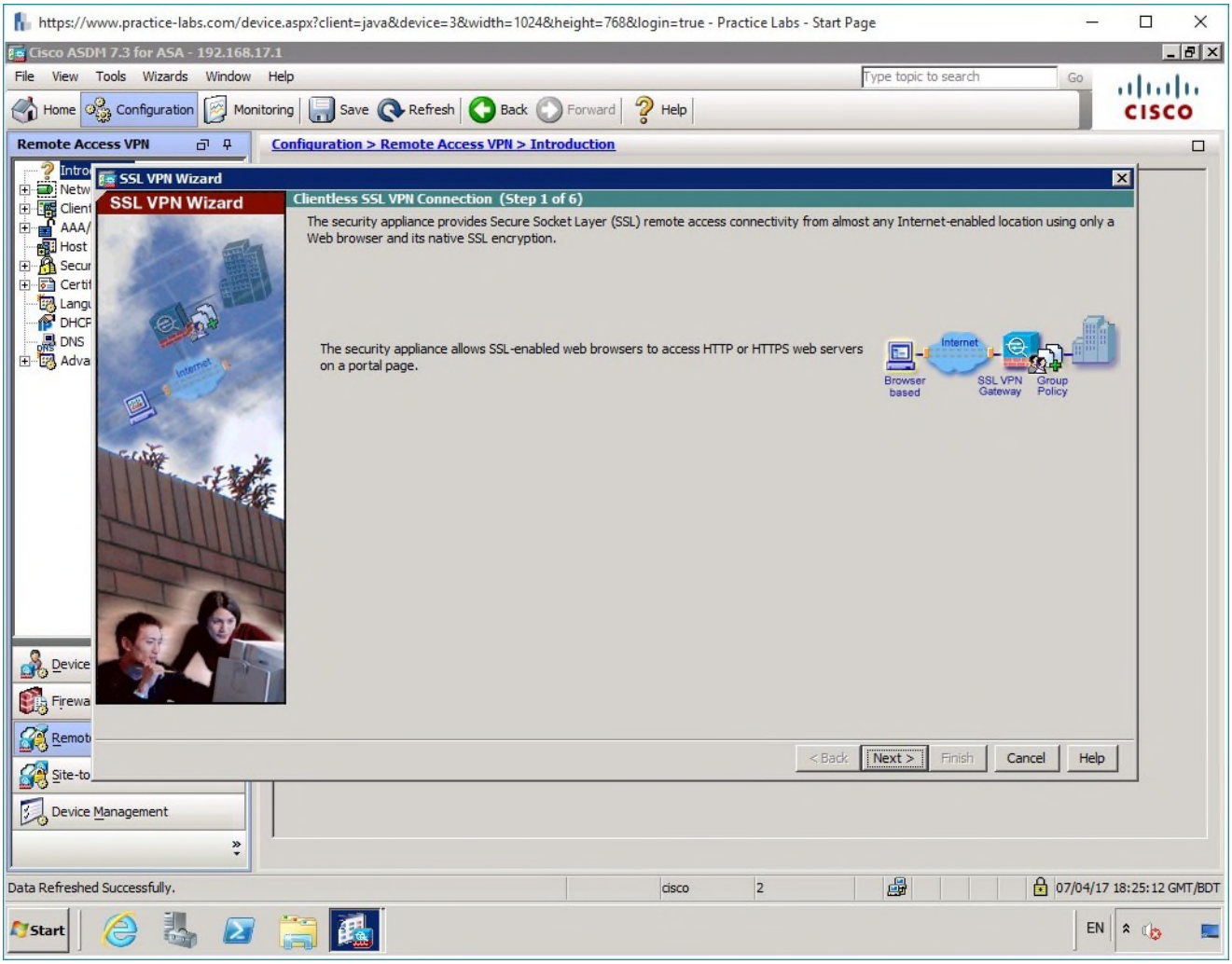


Figura 1.5 Captura de pantalla del Asistente para VPN SSL invocada: Después de hacer clic en Asistentes (Asistentes para VPN SSL, se muestra el Asistente para VPN SSL. Ésta es la primera página, Conexión VPN SSL sin cliente (paso 1 de 6), del asistente.

Step 3

A continuación, tenemos que darle a la VPN SSL un nombre de perfil, llámelo **CLIENTLESS.**

Asegúrese de que la interfaz SSL VPN esté establecida **en Internet.**

Deje el resto de la configuración como predeterminada y haga clic en **Siguiente**.

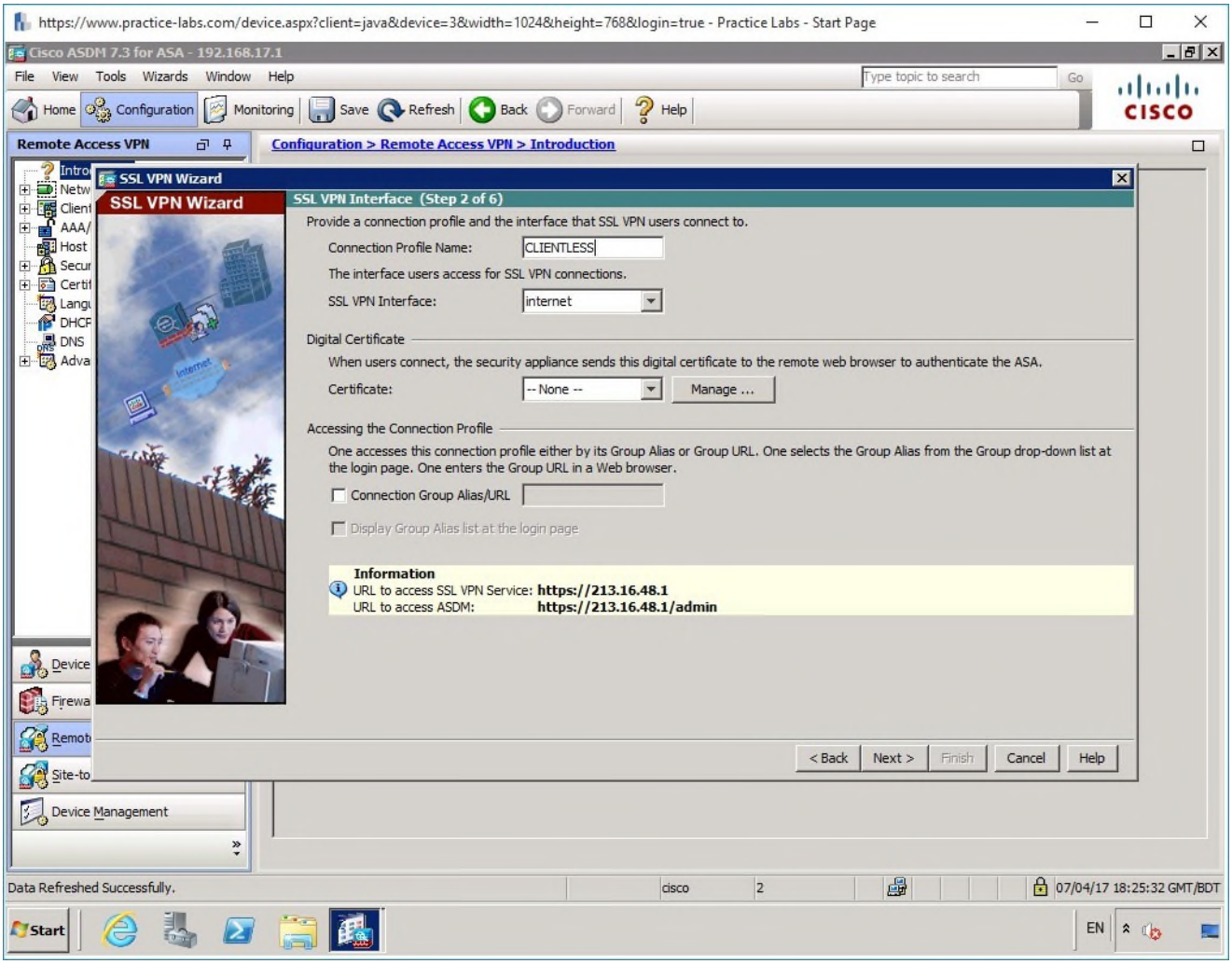


Figura 1.6 Captura de pantalla de la página de la interfaz SSL VPN (paso 2 de 6) del asistente ssl VPN interface: se muestra la página. En la página, se muestran varios campos con sus valores. La sección "Información" visualiza el "URL para acceder el servicio SSL VPN" y los campos "URL para acceder el ASDM" con sus valores se visualizan.

Step 4

En la página de la **autenticación de usuario,** haga clic el botón de radio para habilitar el acceso a la base de datos de usuario local. En este ejemplo no utilizaremos a un servidor TACACS. En su lugar, crearemos localmente un usuario con el que autenticarnos.

La sección **Usuario que se va a agregar** ahora está habilitada, en esta sección ingrese los siguientes detalles:

- Nombre de usuario: **fred**

- Contraseña: **cisco123**
- Confirme: **cisco123**

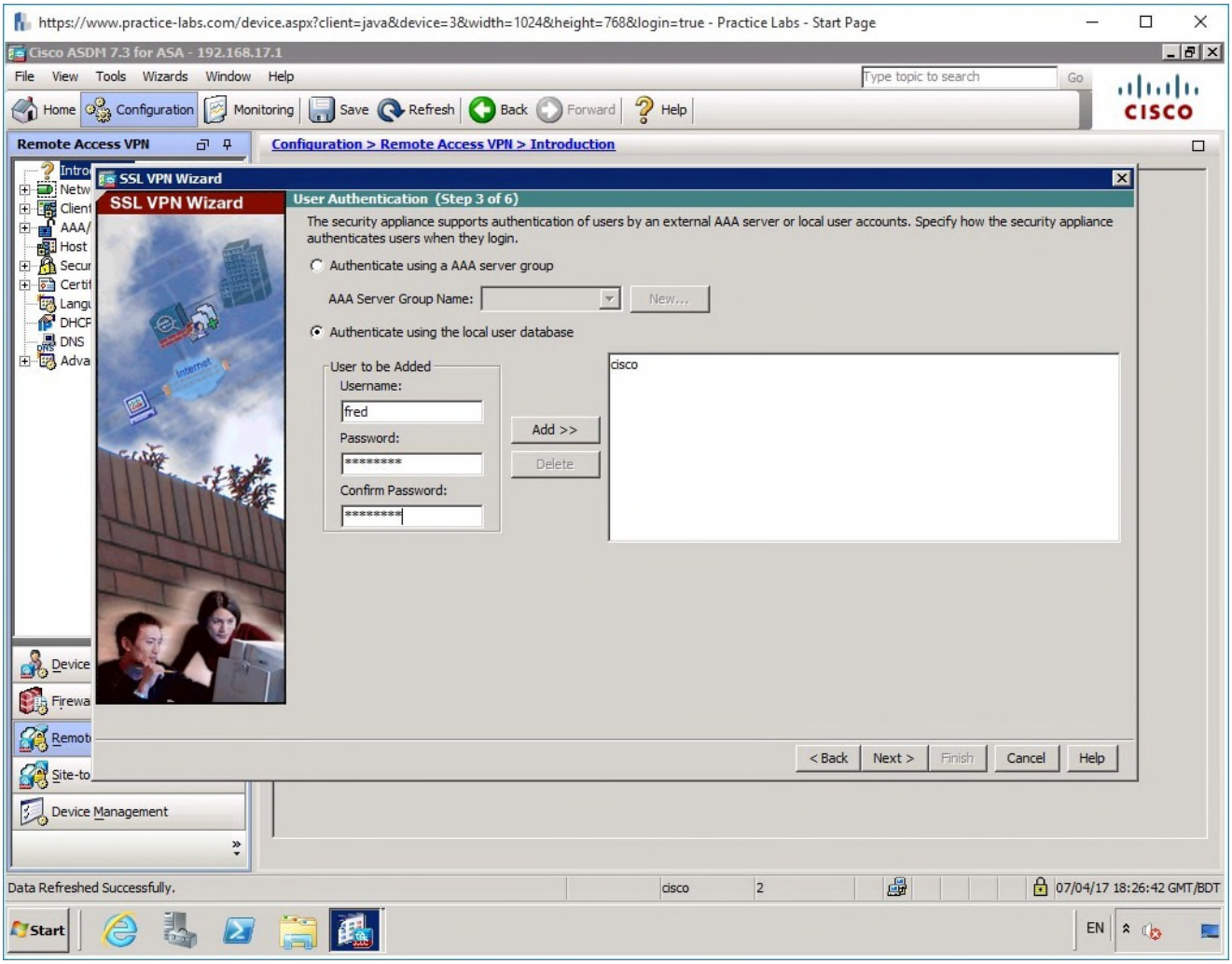


Figura 1.7 Captura de pantalla de la página de autenticación de usuario (paso 3 de 6) del asistente de interfaz SSL VPN: Observe que los campos "Nombre de usuario", "Contraseña" y "Confirmar contraseña" se llenan con los valores respectivos.

Haga clic en **Agregar >>>**

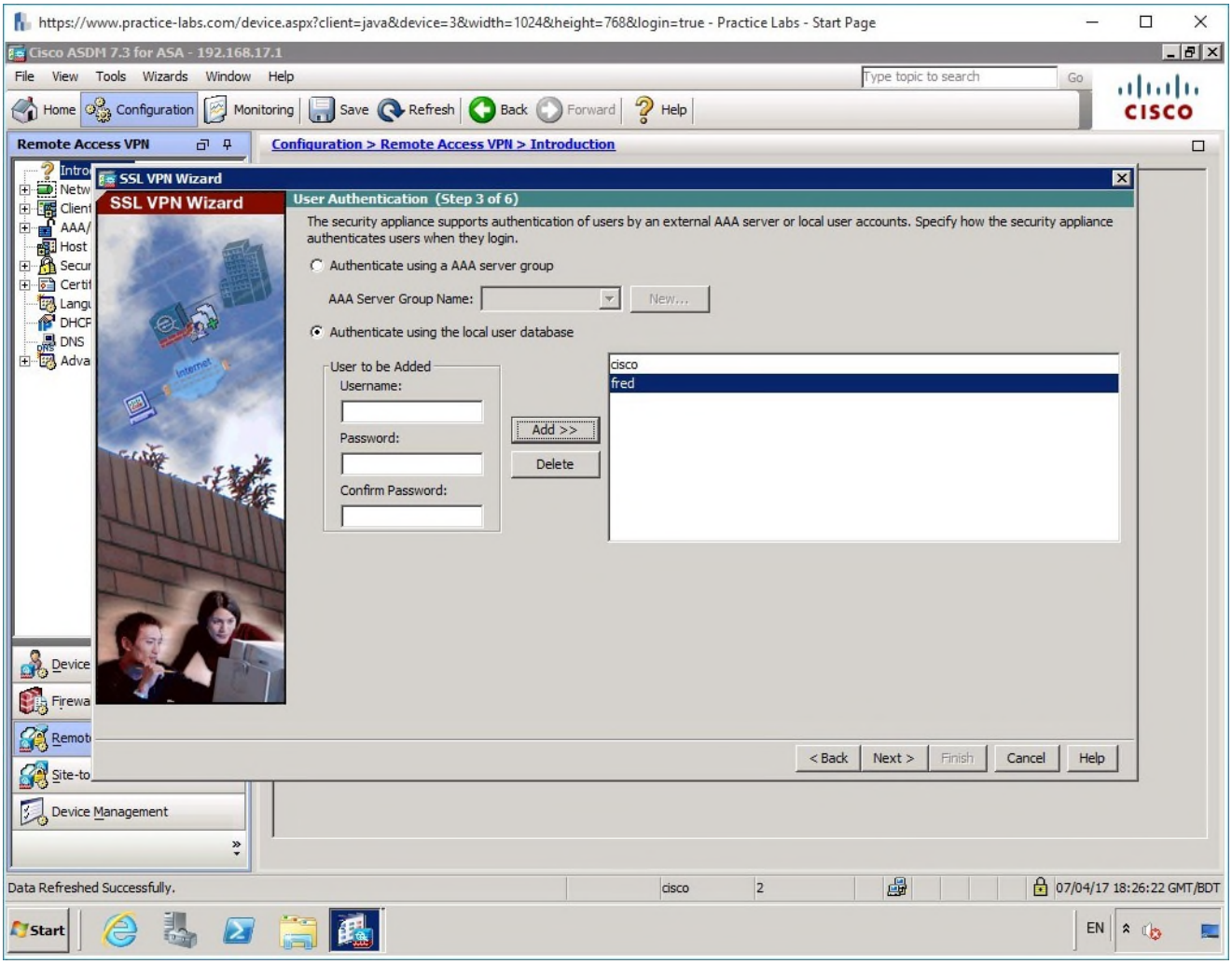


Figura 1.8 Captura de pantalla de la página de autenticación de usuario (paso 3 de 6) del asistente de interfaz SSL VPN: Observe que el nombre de usuario se agrega a la sección derecha.

Haga clic en **Siguiente**.

Step 5

En la página Configuración de directiva de grupo, cree una nueva directiva de grupo denominada **CLIENTLESS_POLICY,** a continuación, haga clic en **Siguiente:**

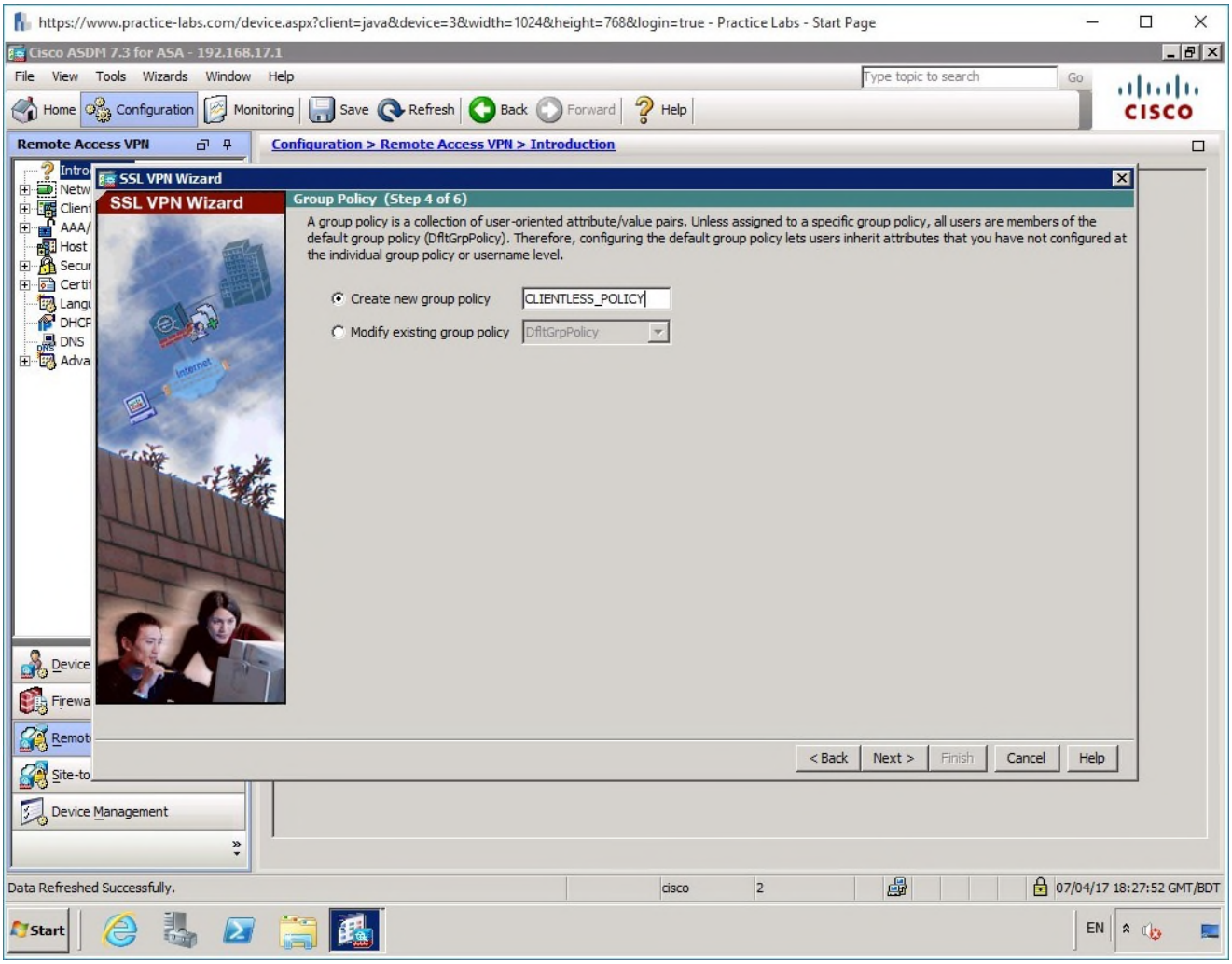


Figura 1.9 Captura de pantalla de la página de directiva de grupo (paso 4 de 6) del Asistente para interfaz VPN SSL: Observe el campo "Crear nueva directiva de grupo" con el valor de CLIENTLESS_POLICY.

Step 6

En la página de lista de marcadores, haga clic en **Administrar**.

El **tecleo agrega** en el cuadro de diálogo de los objetos de la personalización gui de la configuración.

En la página Agregar lista de marcadores, en **nombre,** escriba **mybookmarks**.

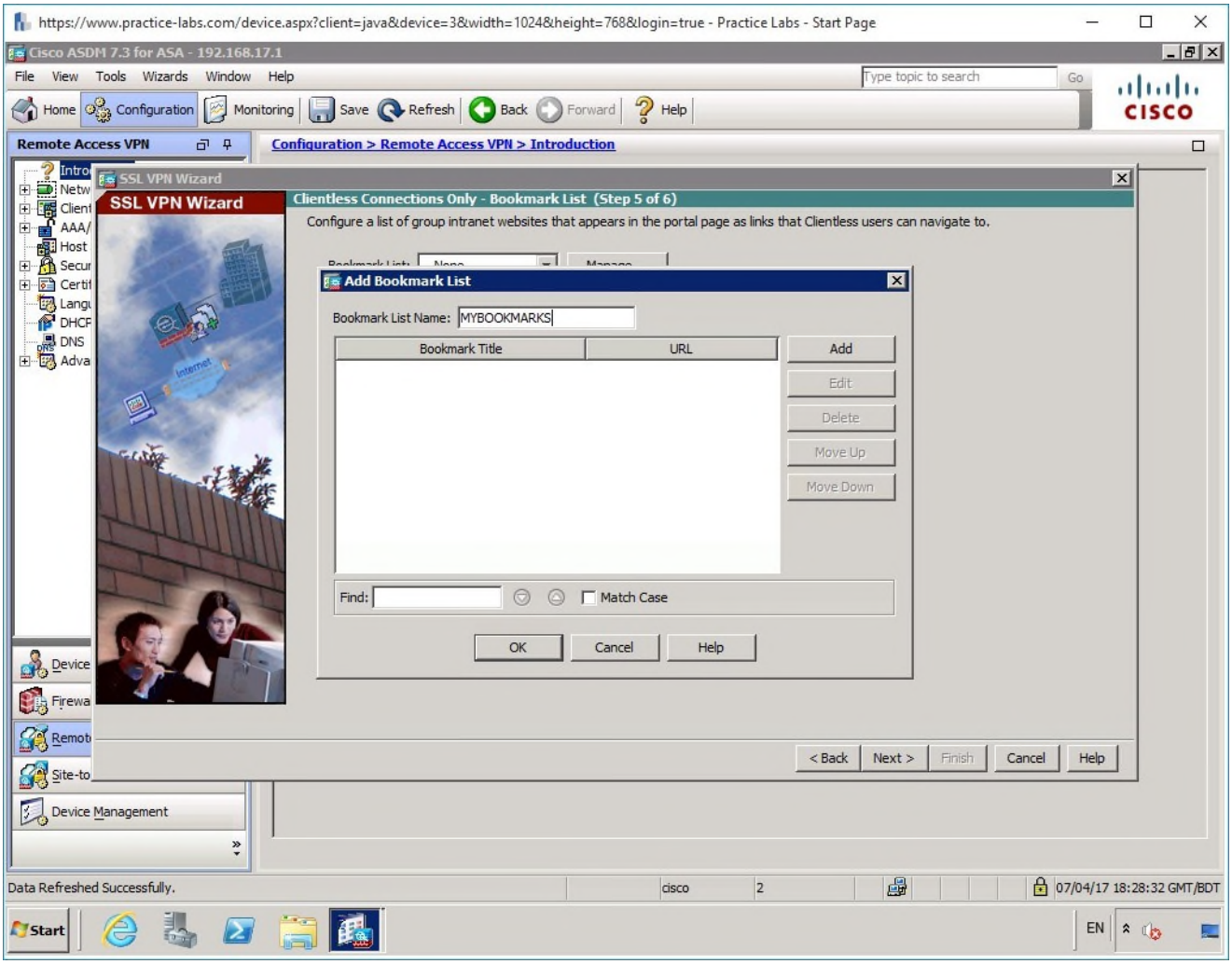


Figura 1.10 Captura de pantalla de la ventana Agregar lista de marcadores: Observe el campo "Nombre de la lista de marcadores" con el valor MYBOOKMARKS.

El **tecleo agrega** a la derecha.

En la página **Tipo de marcador,** deje el valor predeterminado**(URL con el método GET o POST)**y haga clic en **Aceptar**.

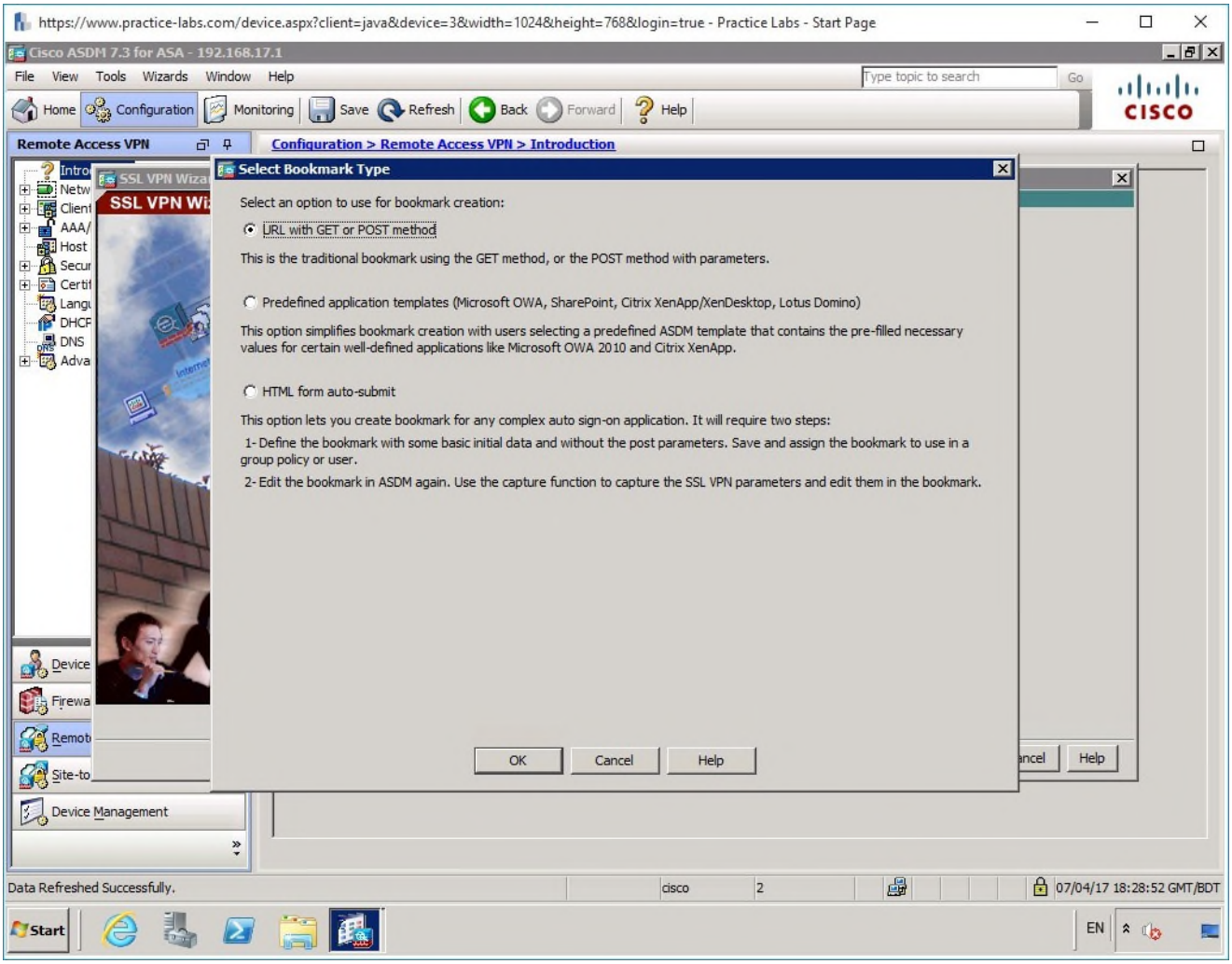


Figura 1.11 Captura de pantalla de la ventana Seleccionar tipo de marcador: Observe la selección de url con el método GET o POST.

En la página **Agregar marcador,** escriba la siguiente configuración:

- Título: **DMZ_WEB**
- Dirección URL: **PLABDMZWEB**

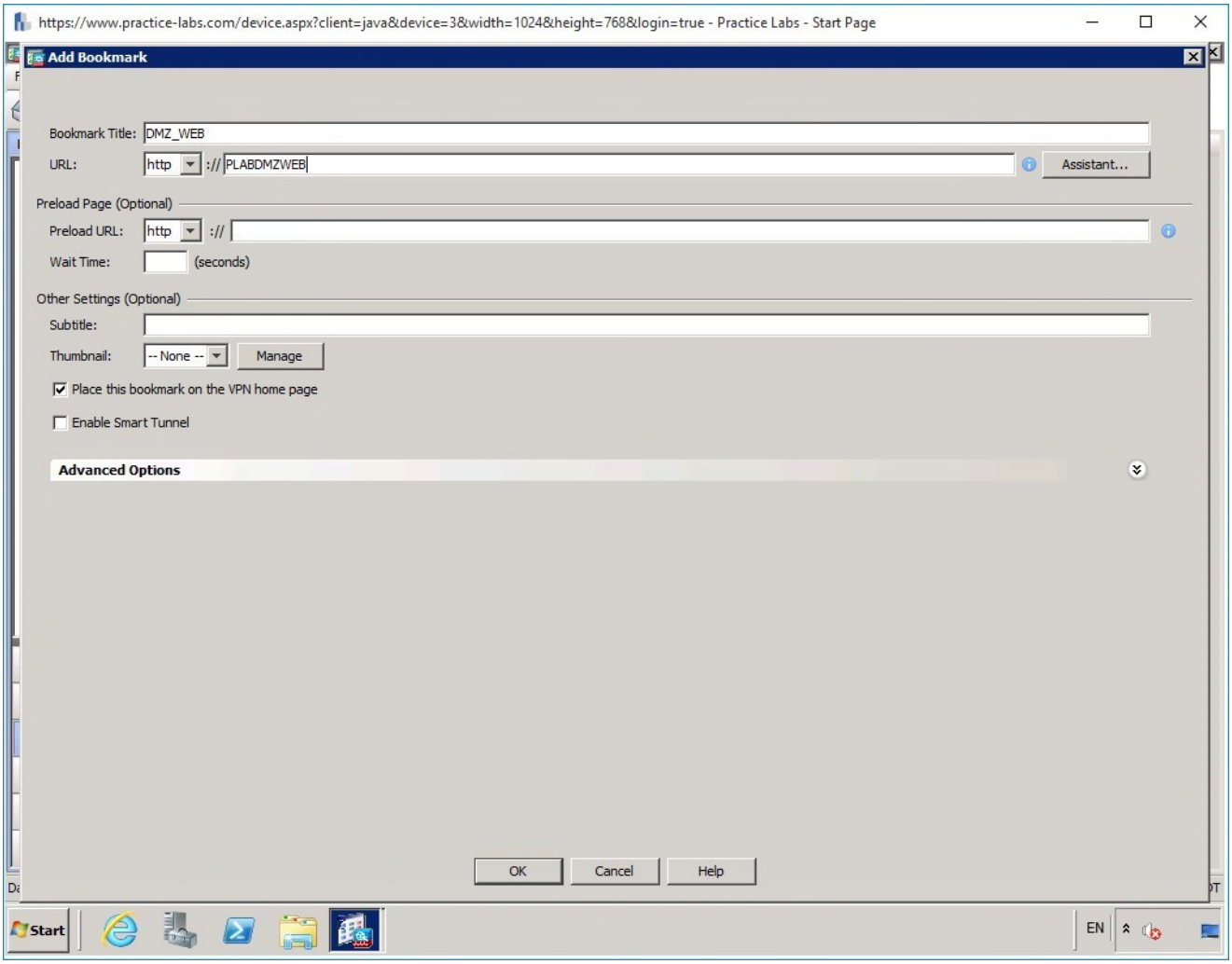


Figura 1.12 Captura de pantalla de la ventana Agregar marcador: Observe el "Título del marcador" con el valor de DMZ_WEB y el campo "URL" con el valor PLABDMZWEB.

Haga clic en **Aceptar**.

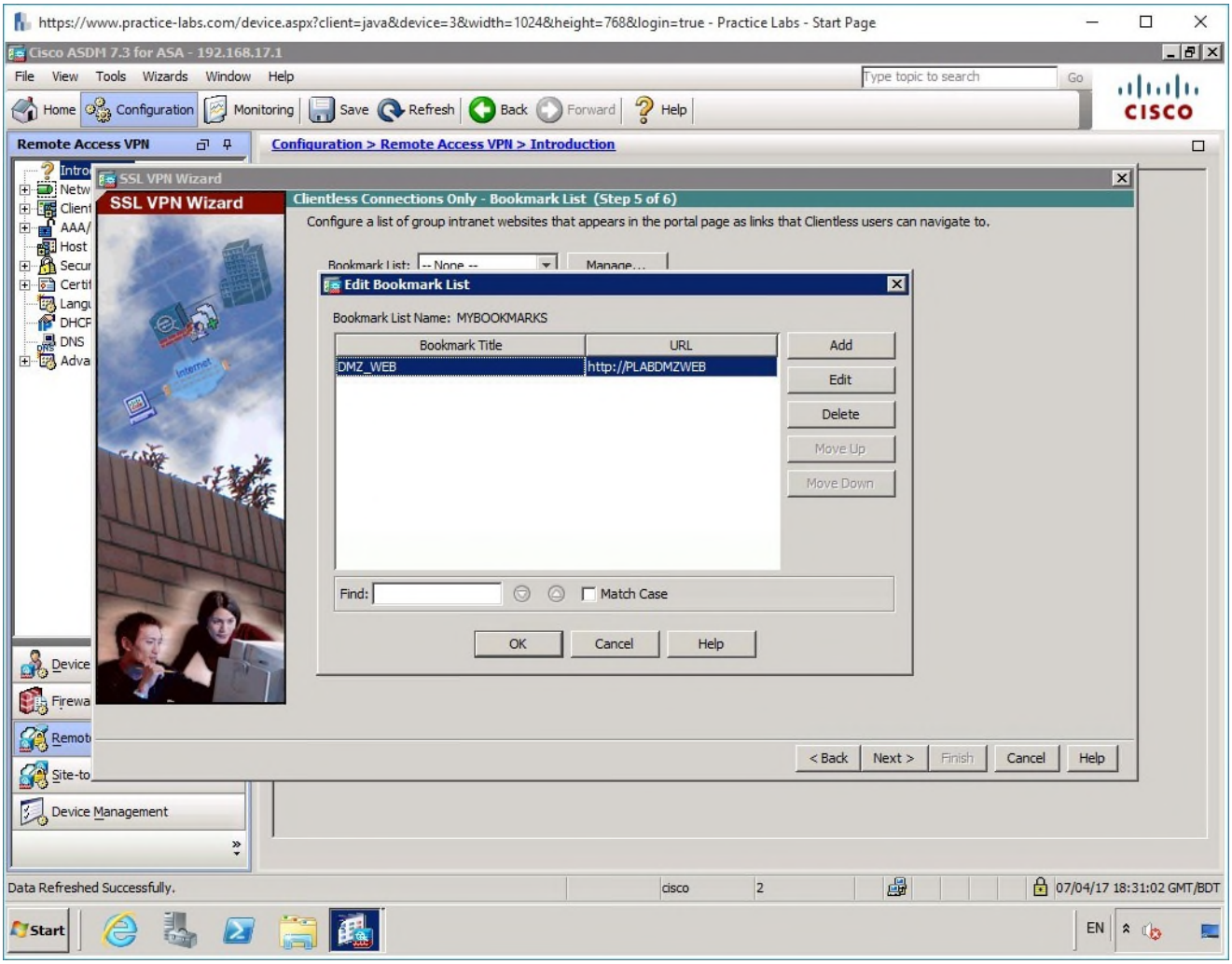


Figura 1.13 Captura de pantalla de la ventana Agregar lista de marcadores: observe los valores de adición en las columnas "Título del marcador" y "DIRECCIÓN URL".

Haga clic en **Aceptar** de nuevo y, a continuación, en **Aceptar** de nuevo en **Configurar objetos de personalización de GUI.**

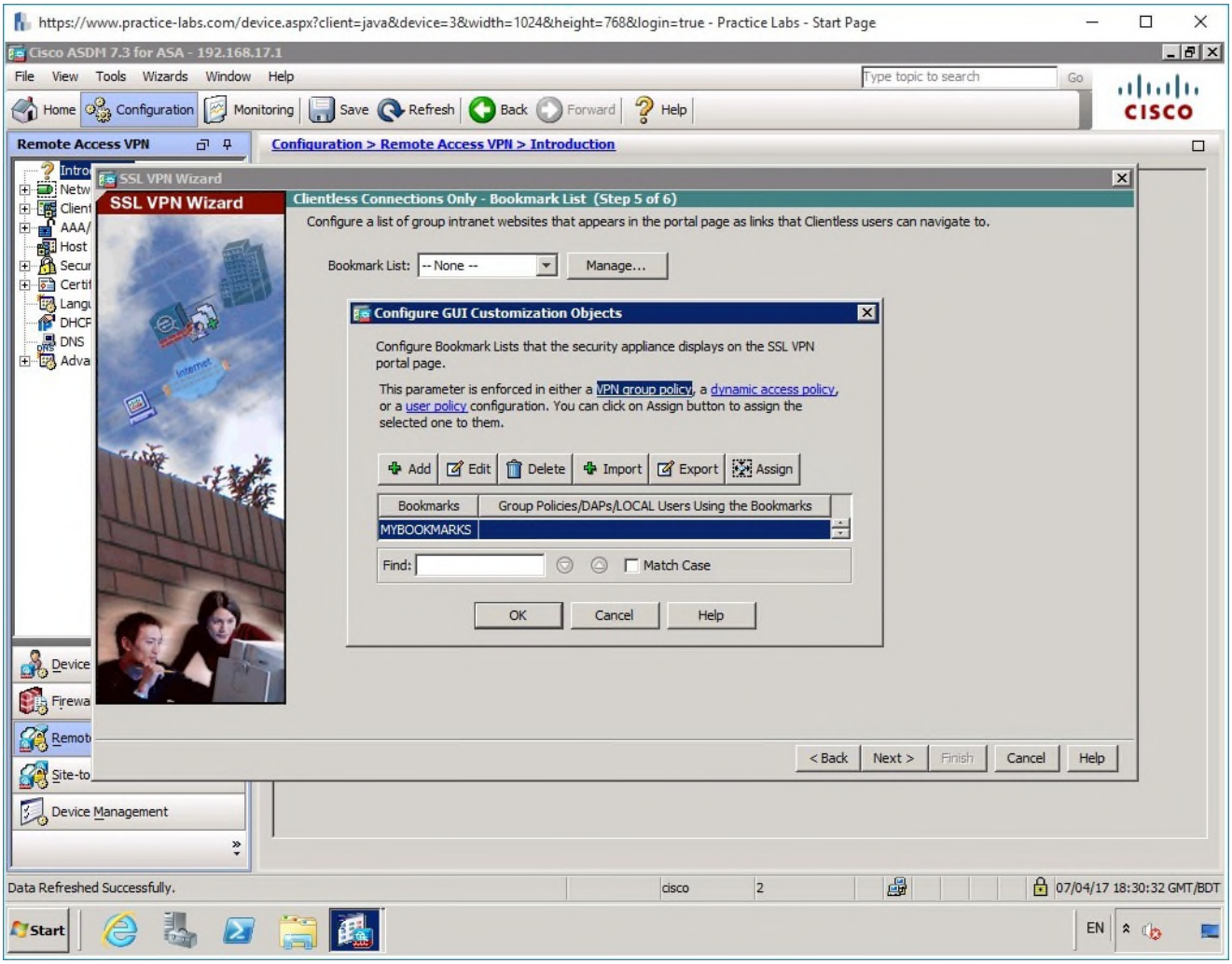


Figura 1.14 Captura de pantalla de la ventana Configurar objetos de personalización de GUI: Observe la adición del valor MYBOOKMARKS.

Finalmente, haga clic en **Siguiente** de nuevo en la página de lista de marcadores:

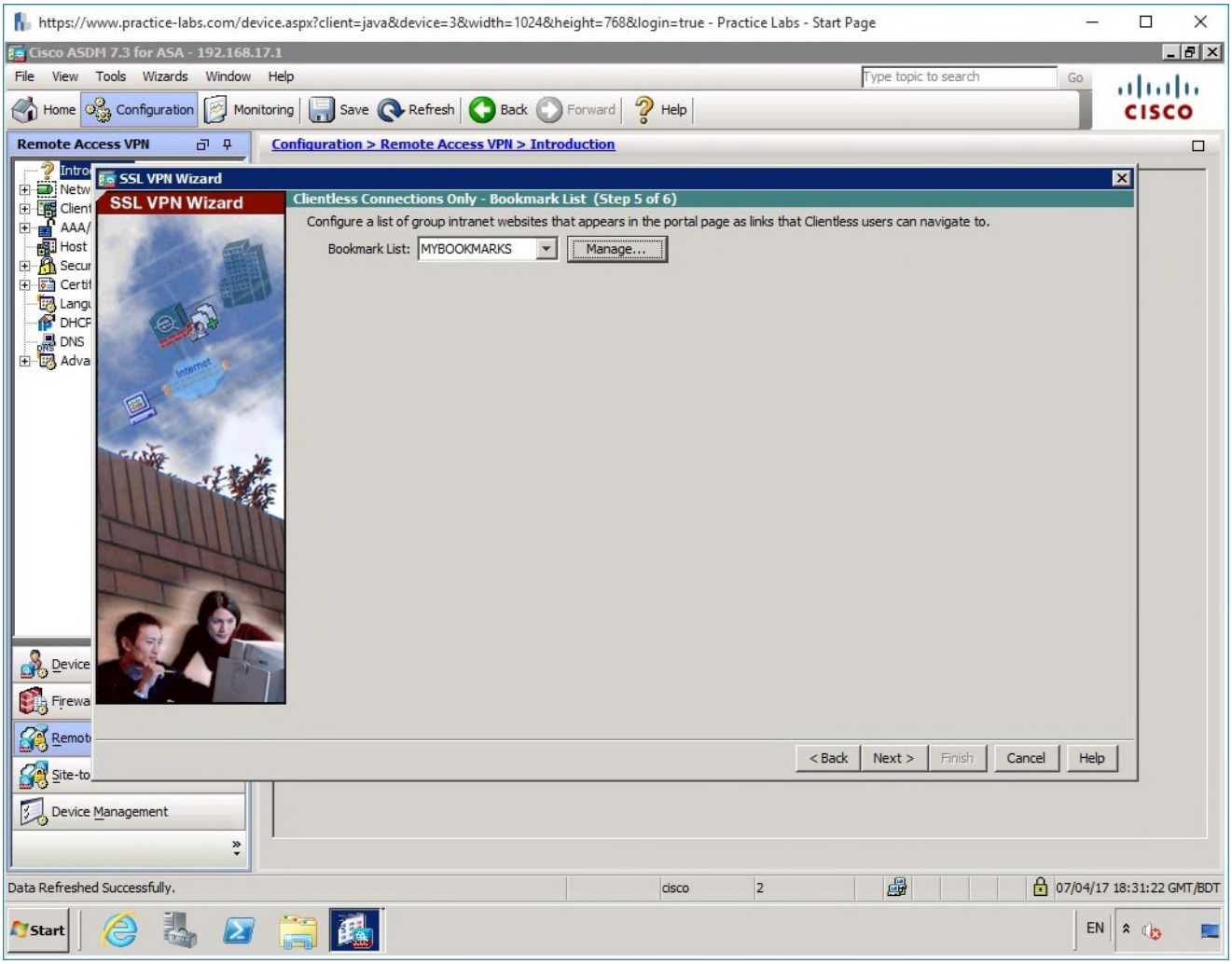


Figura 1.15 Captura de pantalla de la ventana Solo conexiones sin cliente - Lista de marcadores (paso 5 de 6): Observe la selección del valor MYBOOKMARKS en el campo "Lista de marcadores".

Haga clic **en Finalizar** para completar el asistente:

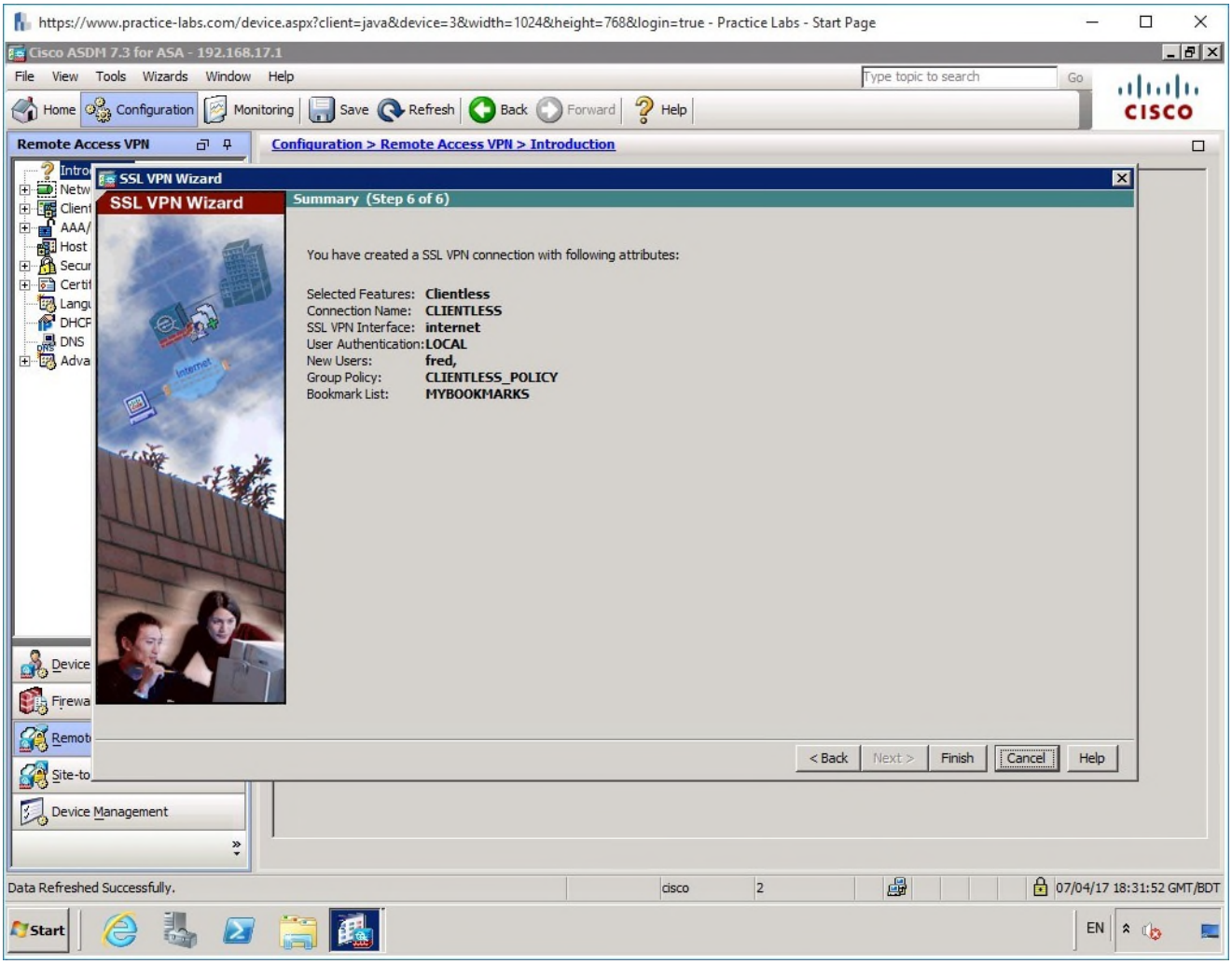


Figura 1.16 Captura de pantalla de la ventana Resumen (paso 6 de 6): Observe la lista de configuración realizada en este asistente.

La configuración será aplicada al ASA, aviso usando el asisitente que usted no tiene que aplicar la configuración, la aplica automáticamente.

Step 7

Una vez completado, conecte con el escritorio de **PLABEXTCLI** entonces usando el **Internet Explorer,**hojee al ASA en **https://213.16.48.1**

Puede tardar un minuto, pero obtendrá un error de certificado, esto está bien en el entorno de laboratorio, ya que no configuramos ningún certificado válido.

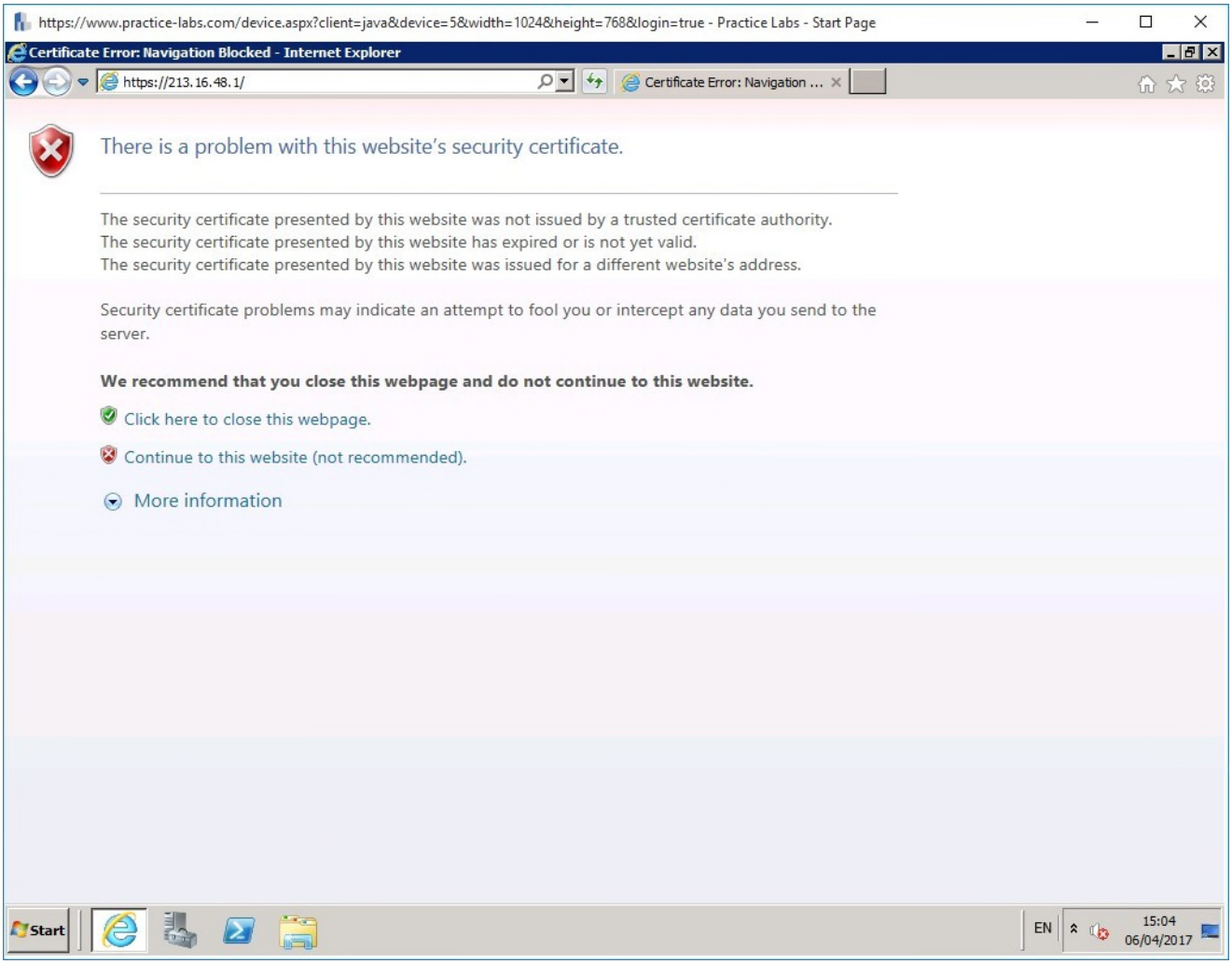


Figura 1.17 Captura de pantalla de Internet Explorer que muestra la dirección URL de http://213.16.48.1: la página web muestra el problema con el certificado de seguridad.

El **tecleo continúa a este Web site (no recomendado)** y la página de inicio de sesión ASA aparecerá:

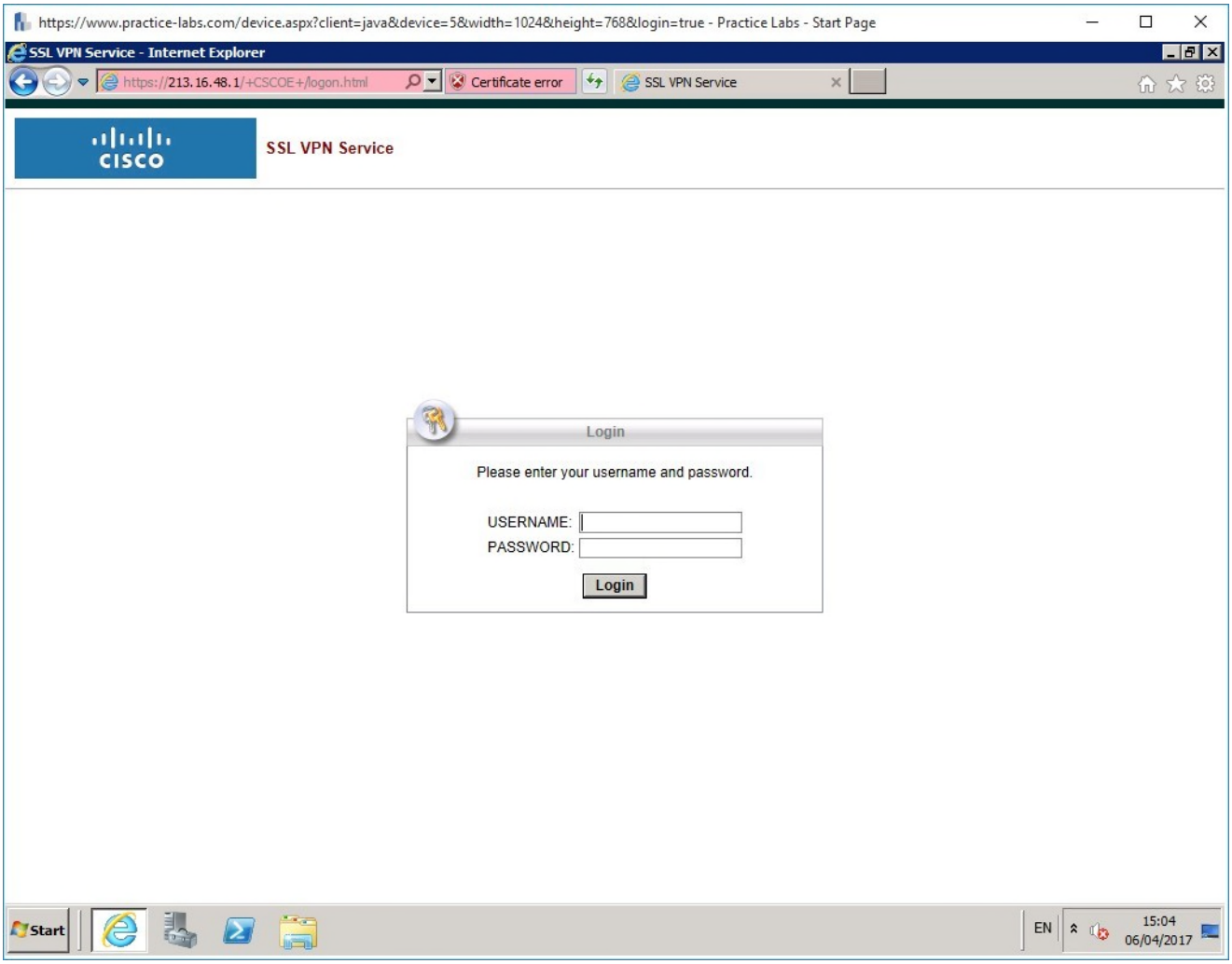


Figure 1.18 Screenshot of initial SSL VPN Service login window: This is window on which a user needs to enter the user credentials.

Login with the username that you created, **fred** and the following password:

```
cisco123
```

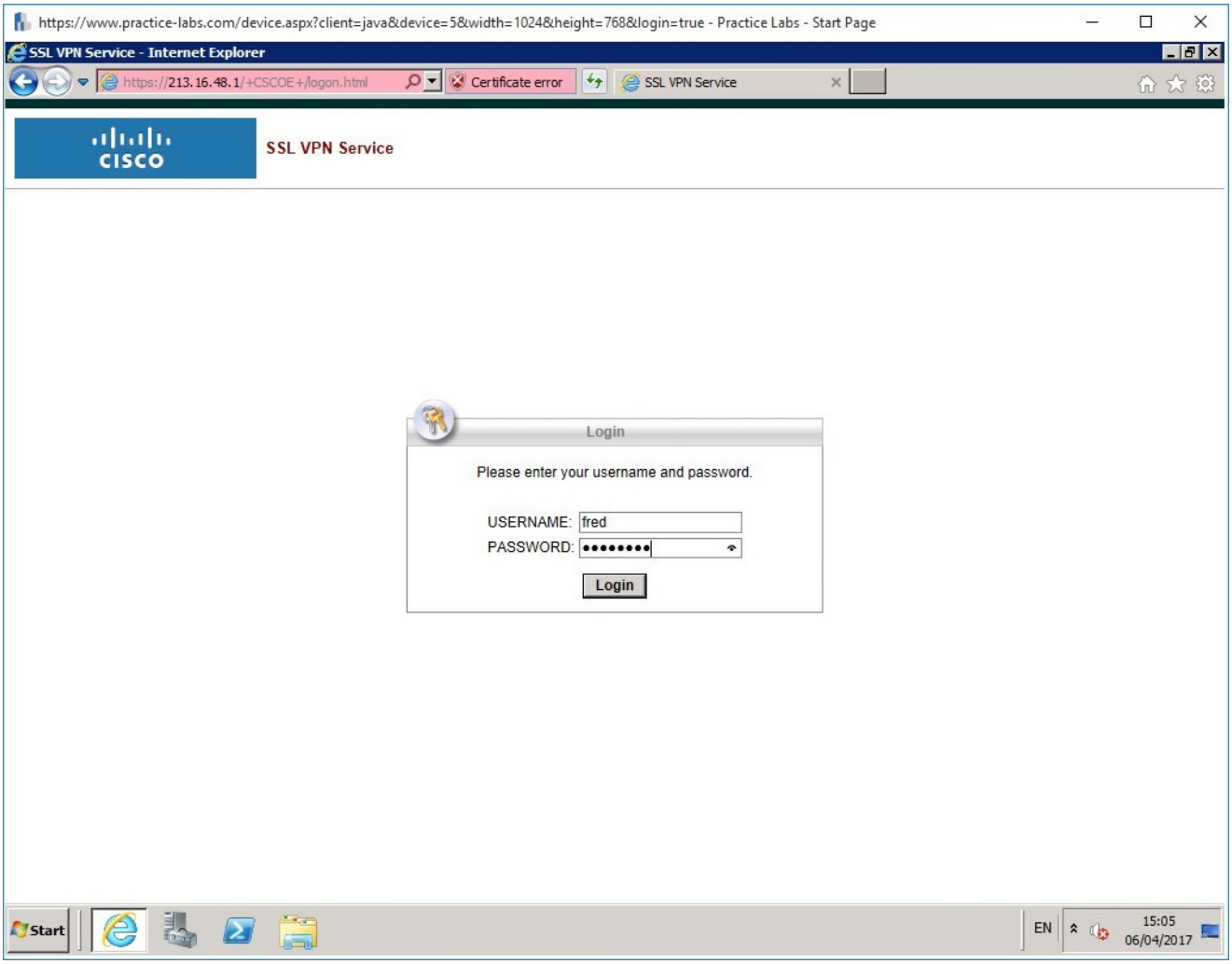


Figure 1.19 Screenshot of SSL VPN Service login window with credentials: Notice the values in the “USERNAME” and “PASSWORD” fields.

Step 8

Once logged in you will see the bookmark that you created previously:

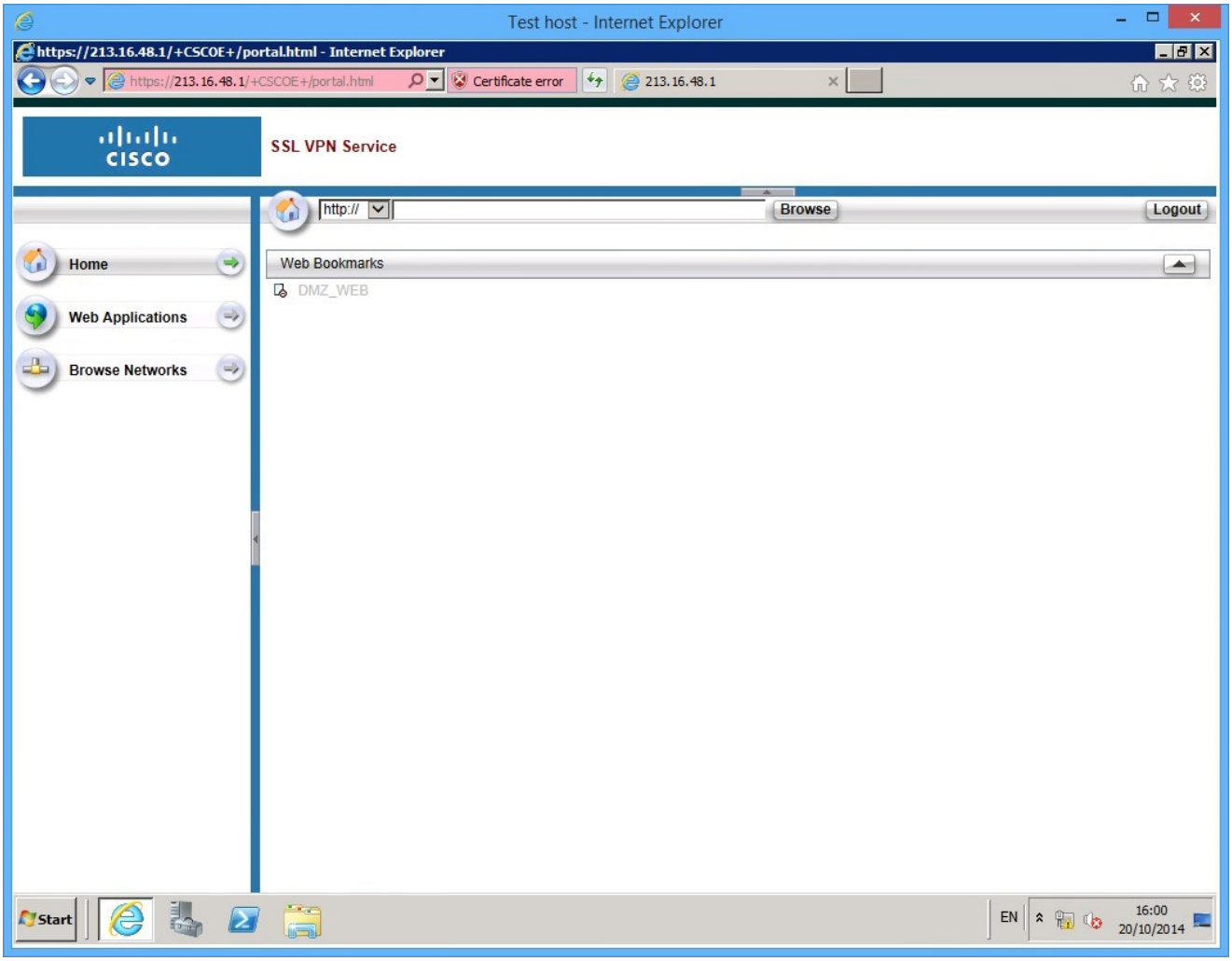


Figure 1.20 Screenshot of homepage of SSL VPN Service Web application: After the username and password are entered and successful authentication, the home page of SSL VPN Service Web application is displayed.

However, notice that this is greyed out if you hover over the link it will explain why. We need to add a host entry in for this server as the ASA cannot resolve the address.

Step 9

Connect to the LDNFWASA01. Use the following command to add a name:

```
LDNFWASA01# configure terminal
LDNFWASA01(config)# name 172.16.16.10 PLABDMZWEB
```

If you flip back to **PLABMGMT,** you will notice that the ASDM is showing an **ASDM out of sync** message. Whenever you configure something on the CLI and have the ASDM software open, this message will appear, you can just click **Refresh Now** to tell the ASDM to pull the latest configuration.

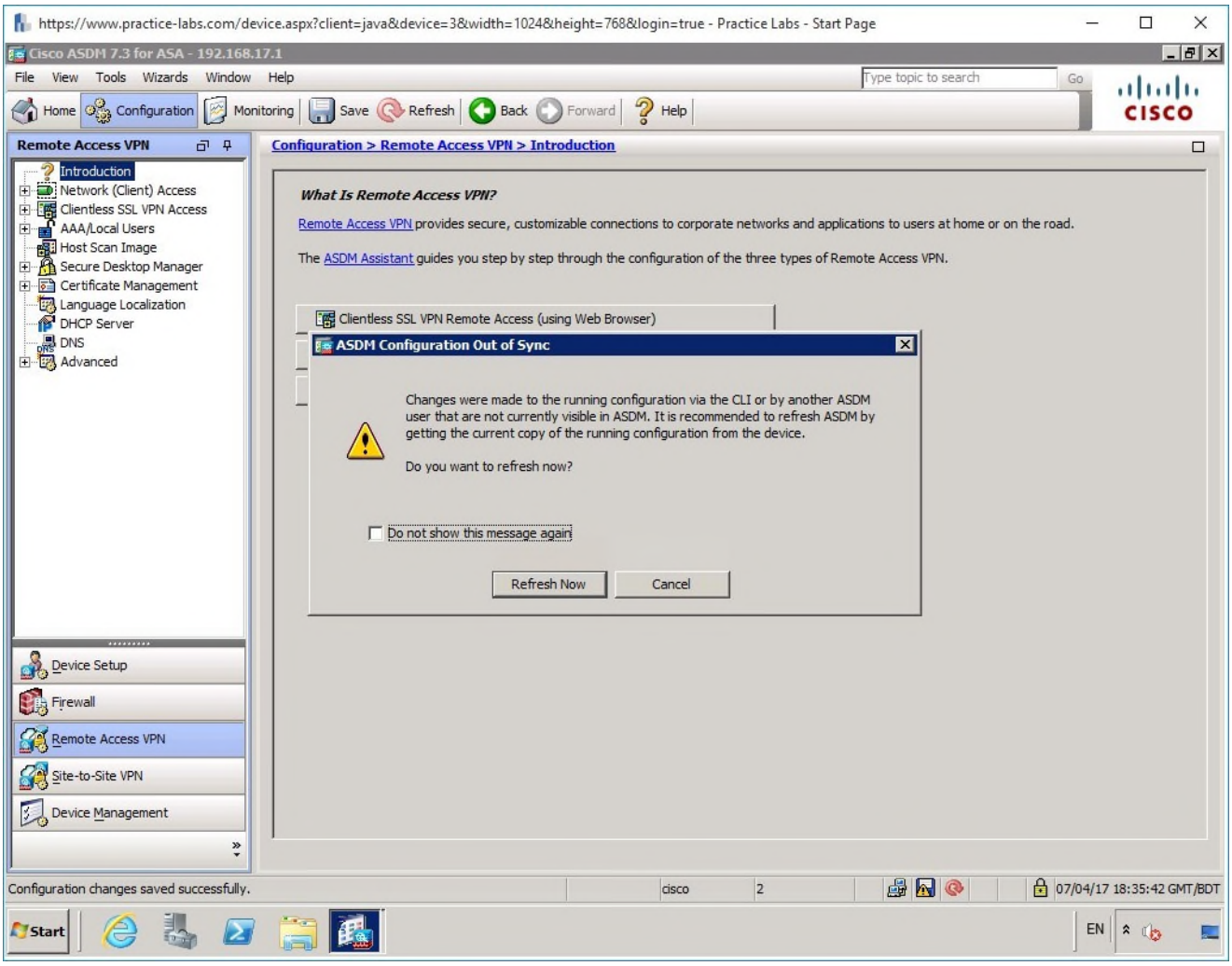


Figure 1.21 Screenshot of Out of Sync: A prompt displaying a message to refresh ASDM.

> ***Note:*** *In a production environment you may want to point your firewalls to an internal DNS server if configuring lots of bookmarks!*

Step 10

Refresh your SSL VPN client page on PLABEXTCLI:

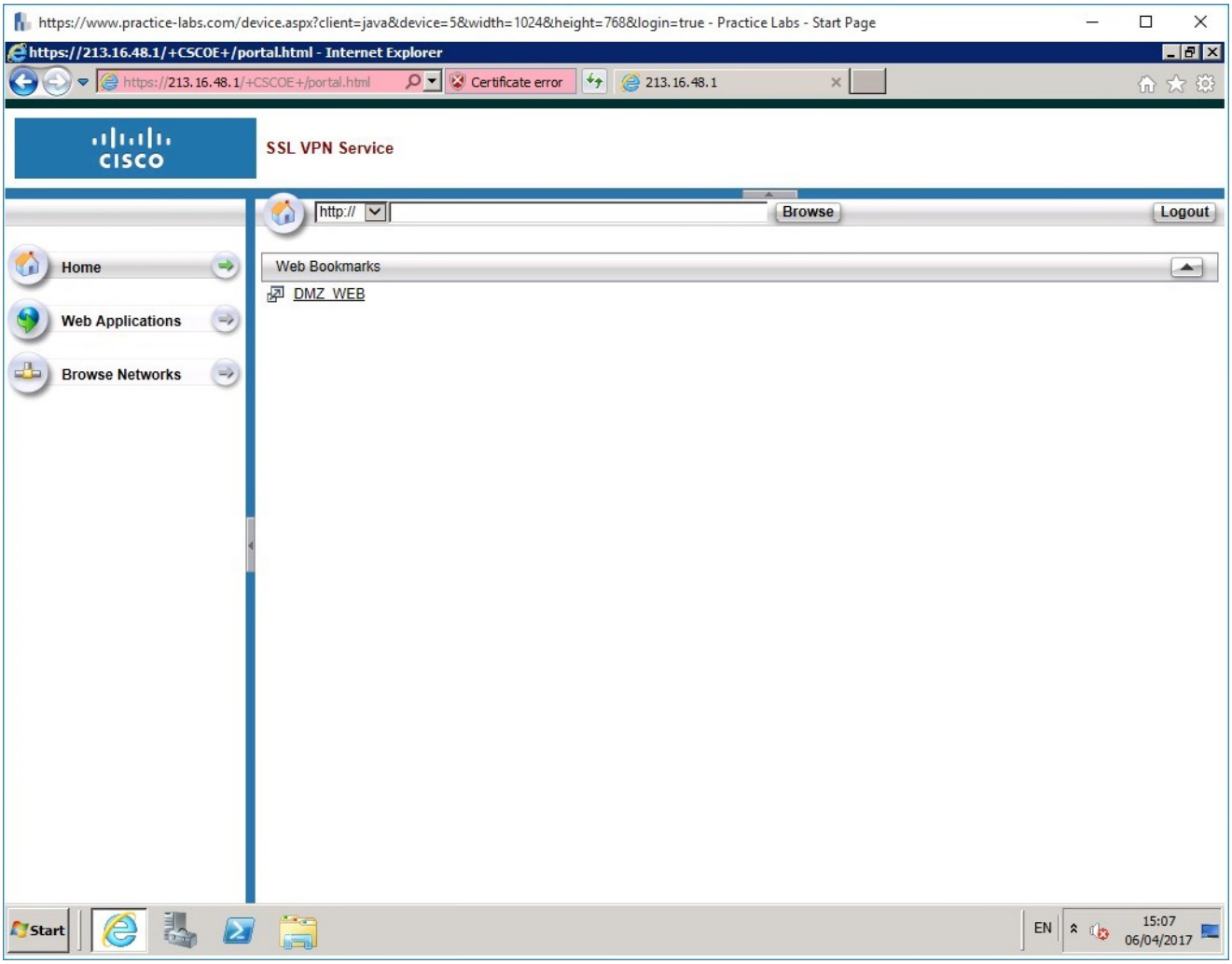


Figure 1.22 Screenshot of initial screen of SSL VPN Service: Notice that the initial screen displays DMZ_WEB.

The link is now clickable. Click the link:

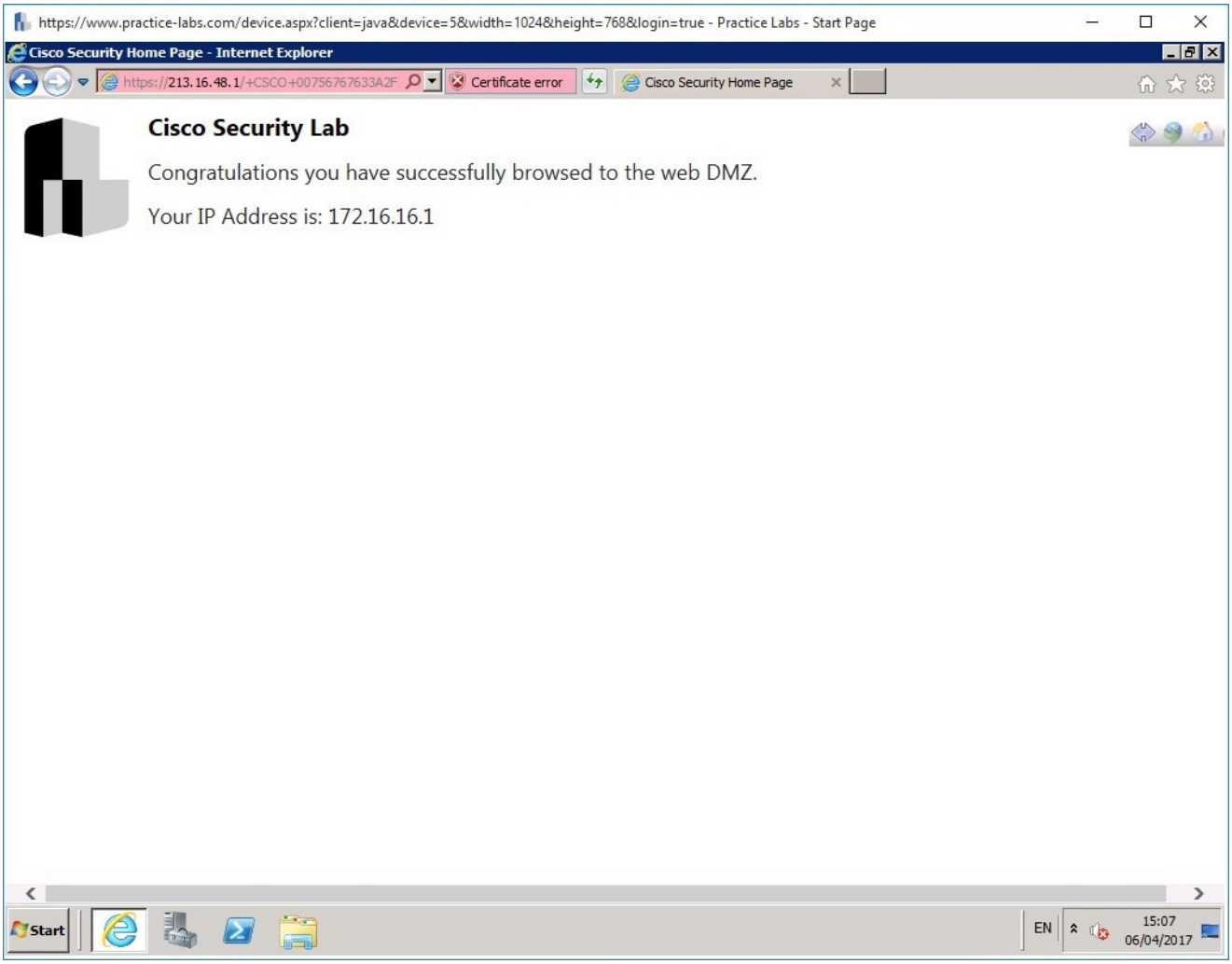


Figure 1.23 Screenshot of initial screen of Cisco Security Lab: Notice that the success message for successfully browsing to the DMZ web. The Webpage also displays your IP address.

Notice how the IP Address is displayed as 172.16.16.1, which is the ASA DMZ interface address! Your SSL VPN is working.

Leave your devices powered on and continue to the next exercise.

Exercise 2 - Implement AnyConnect using the Cisco ASA Device Manager

In this exercise, you will configure the Cisco **AnyConnect** client. In my personal experience, even though you have to download the client to the machine, it is a much better user experience than the Clientless SSL VPN.

Task 1 - Configure the AnyConnect Client

To configure the AnyConnect client, we will use a similar process as before.

Step 1

Firstly, let's just ensure no existing identity key pairs exist.

Connect to the LDNFWASA01 and enter the following commands in **bold** below to zeroize the existing identity keys:

```
LDNFWASA01# configure terminal
```

```
LDNFWASA01(config)# crypto key zeroize rsa
WARNING: All RSA keys will be removed.
WARNING: All device digital certificates issued using these
keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
```

Step 2

Re-login to the ASDM software on **PLABMGMT**, navigate to the menu and click **Wizards > VPN Wizards > AnyConnect VPN Wizard**:

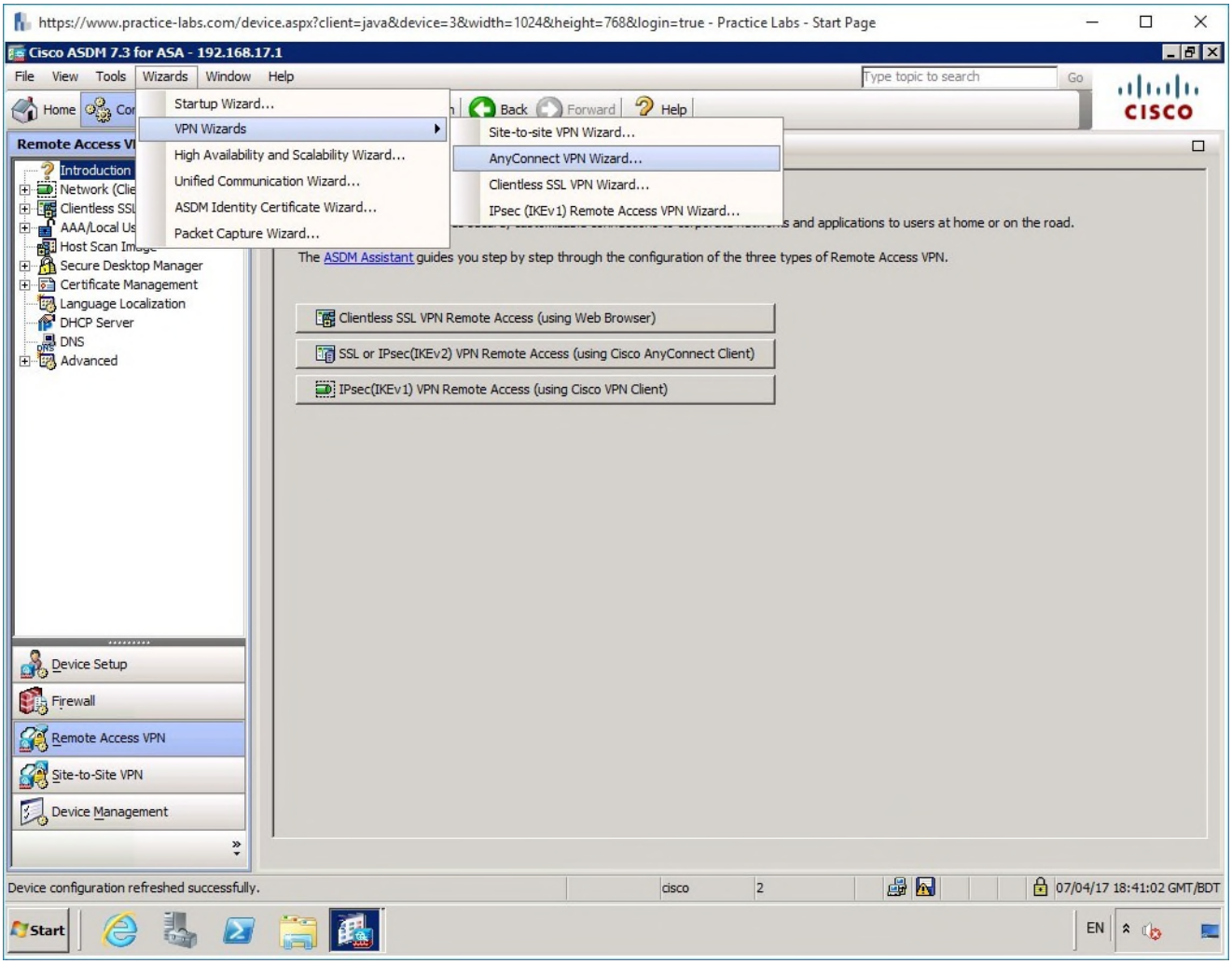


Figure 2.1 Screenshot of initial Cisco ASDM-IDM Launcher configuration window: After clicking Wizards (VPN Wizards menu options, you will see multiple options from which you need to select AnyConnect VPN Wizard.

Click **Next** on the first page:

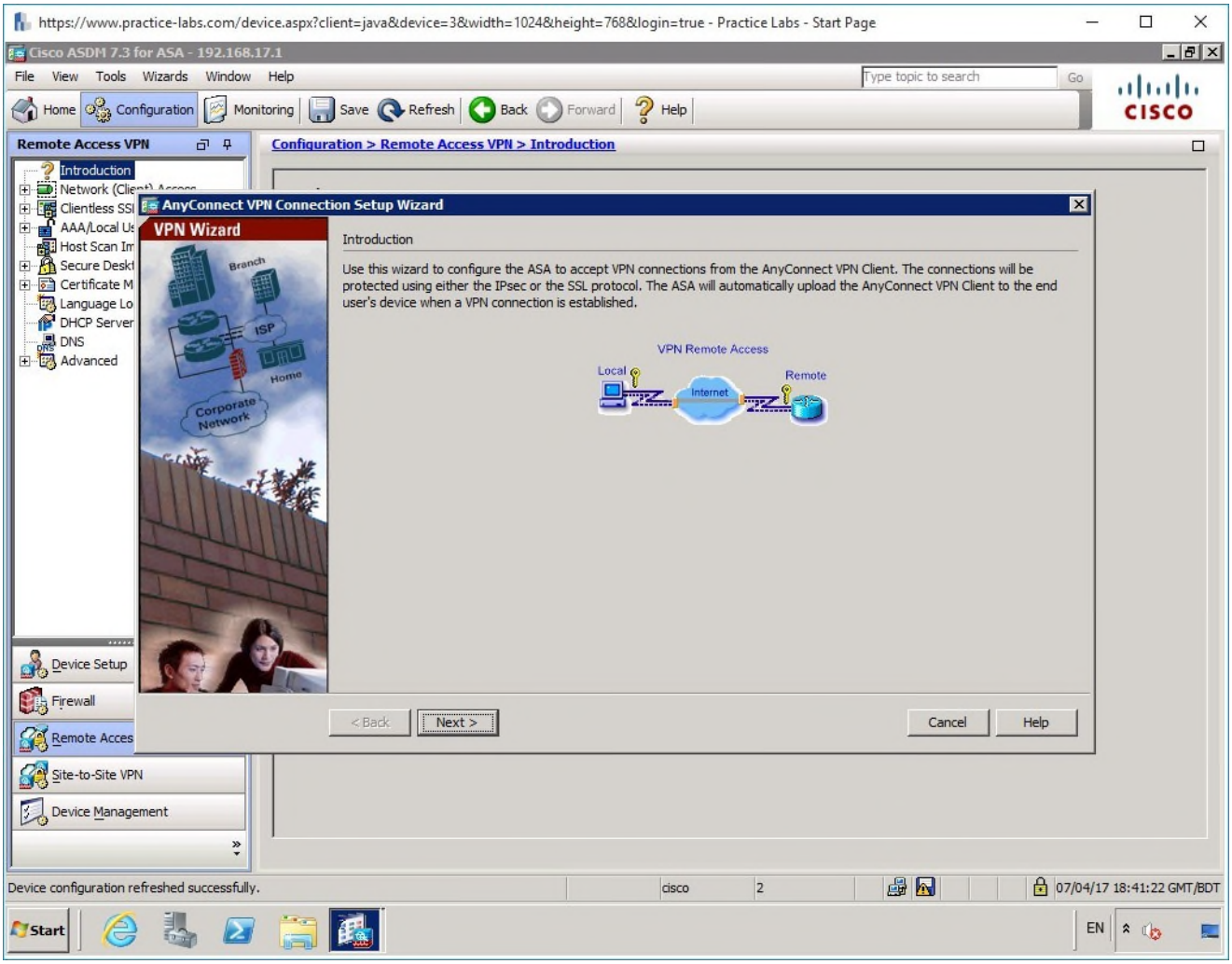


Figure 2.2 Screenshot of AnyConnect VPN Connection Setup Wizard invoked: After clicking Wizards (AnyConnect VPN Wizards, the AnyConnect VPN Wizard is displayed. This is the introduction page.

Step 3

Next, in the **Connection Profile Identification** page enter the profile name as **ANYCONNECT**, ensure the VPN Access Interface is set to **internet**:

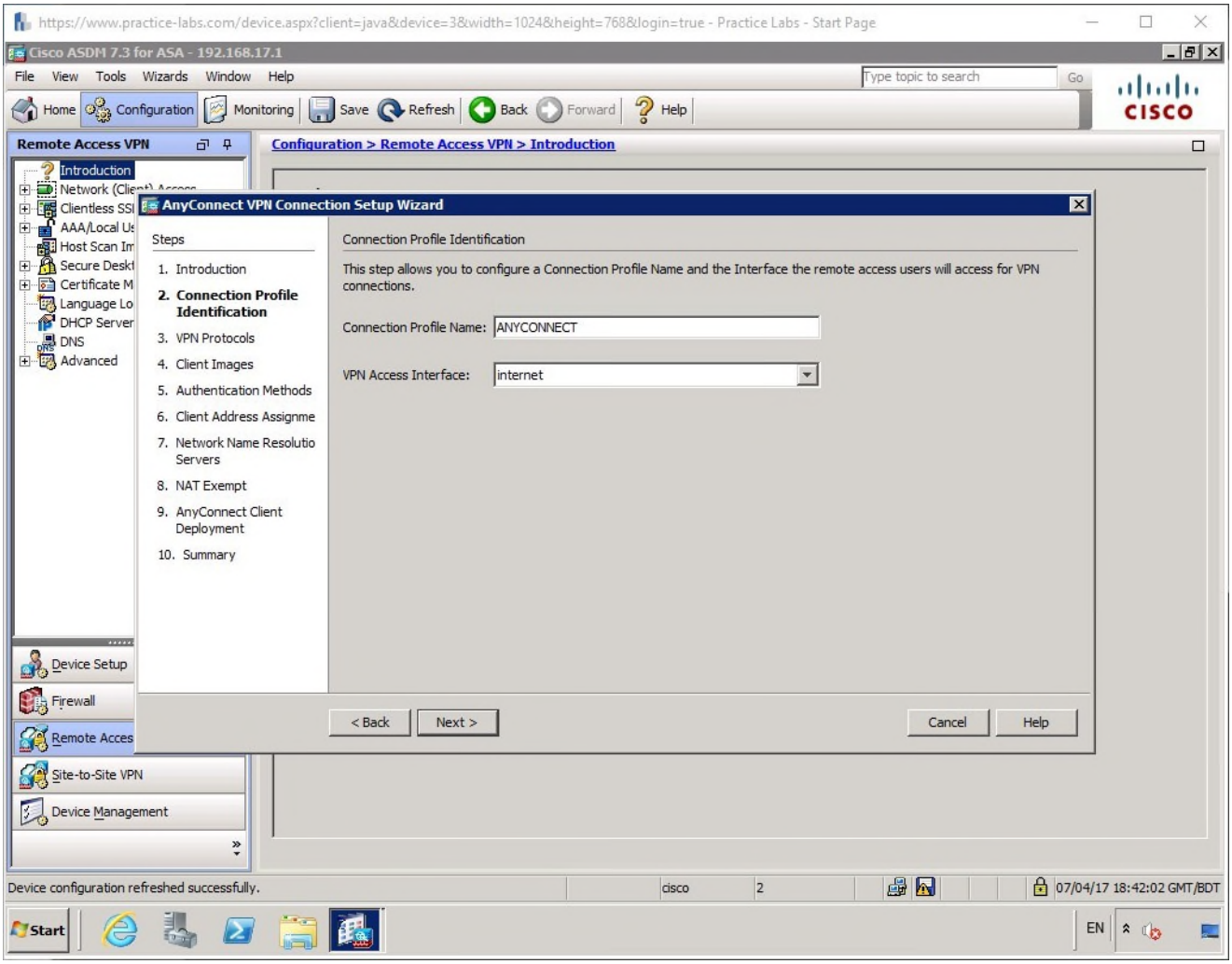


Figure 2.3 Screenshot of the Connection Profile Identification page: The "Connection Profile Name" field displays the ANYCONNECT value and the "VPN Access Interface" field displays the Internet value.

Step 4

On the VPN Protocols page, leave the defaults selected (SSL and IPSec). Click the **Manage** button to generate a self-signed certificate:

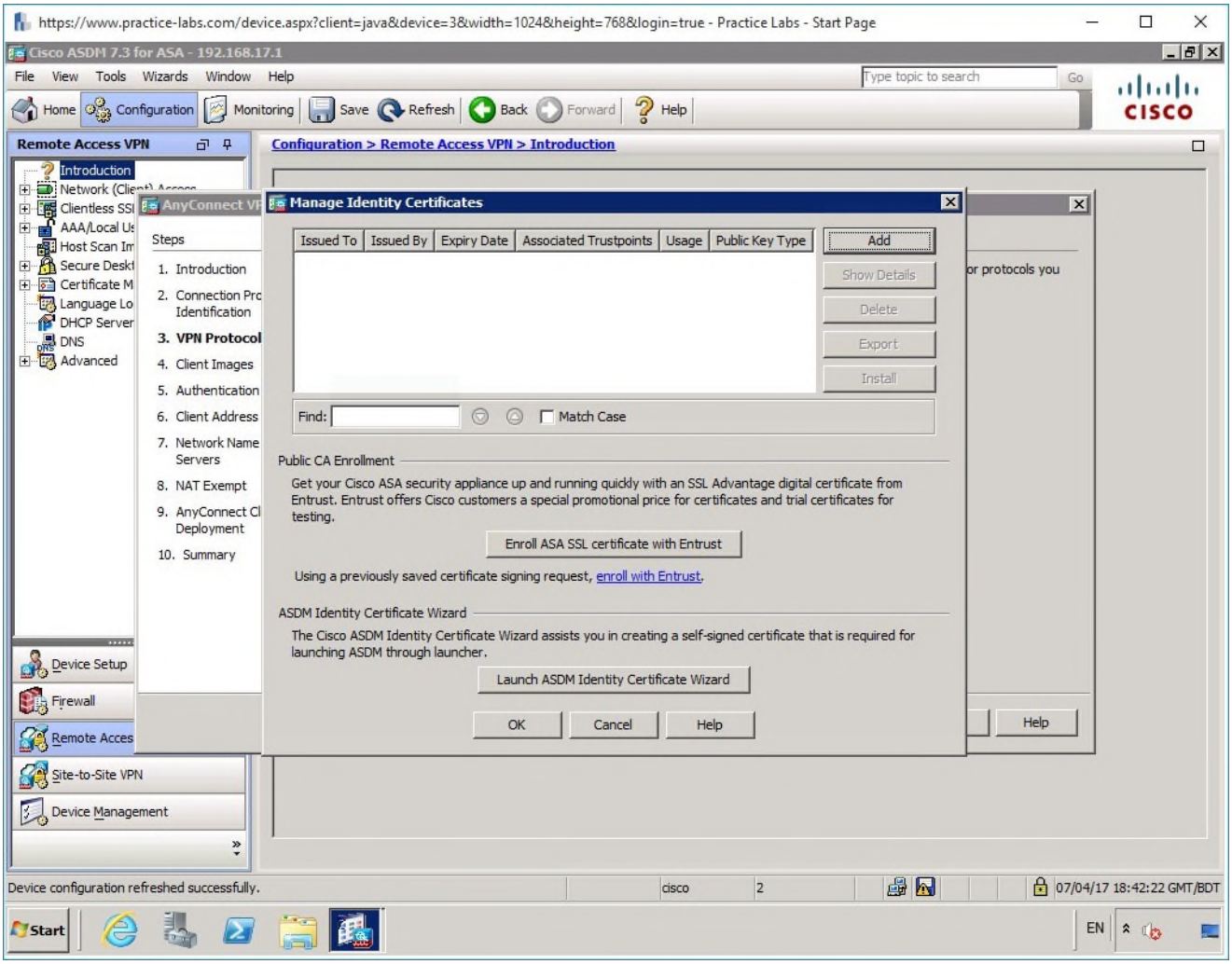


Figure 2.4 Screenshot of the initial Manage Identity Certificates window: User is prompted to add a certificate, which can either be a new identity or self-signed certificate.

Click **Add** in the top right. Ensure you select the following:

- **Add a new identity certificate**
- **Generate self-signed certificate**

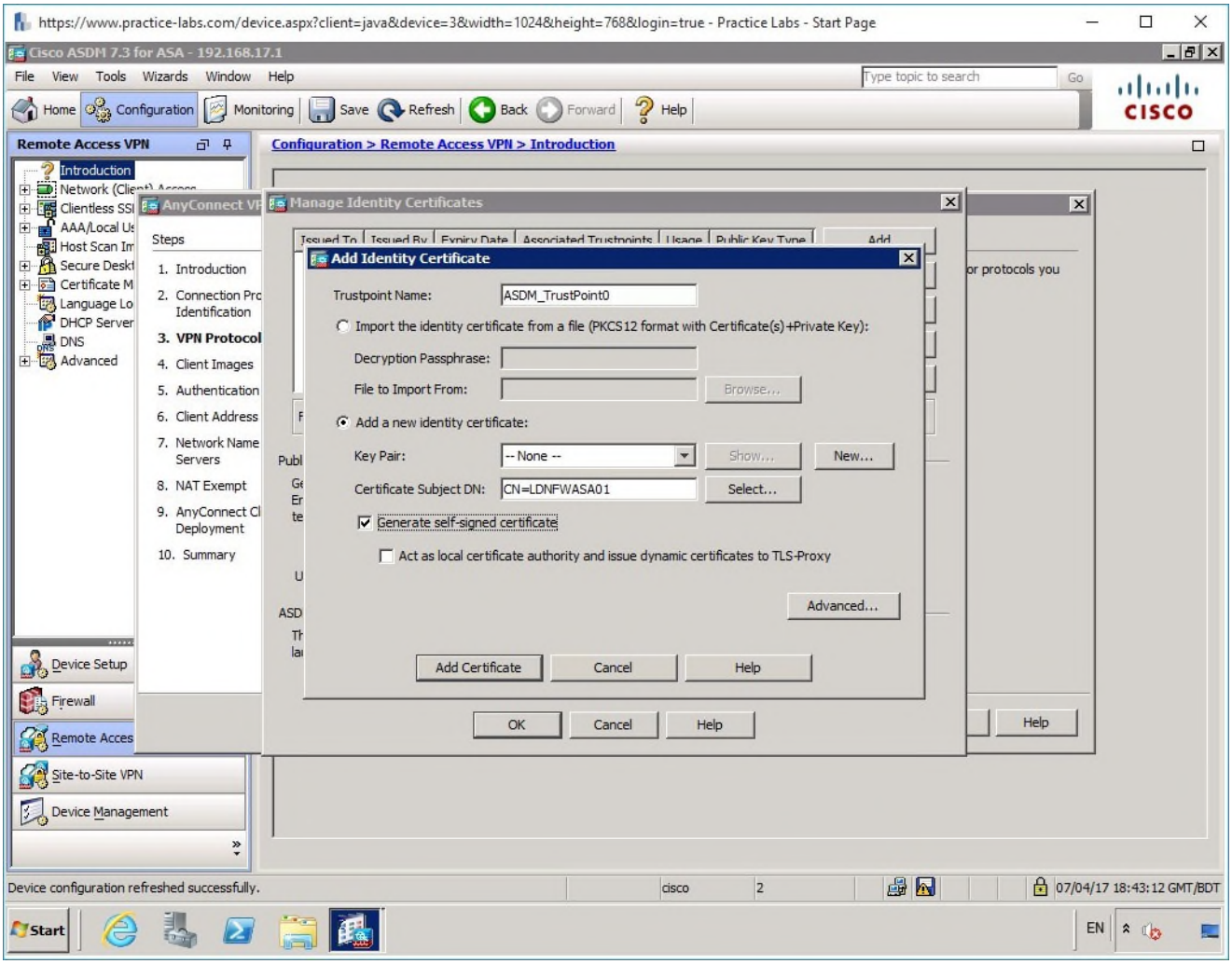


Figure 2.5 Screenshot of the Add Identity Certificate window: User is prompted to create a new key pair.

Click **New** next to the **Key pair** drop down menu:

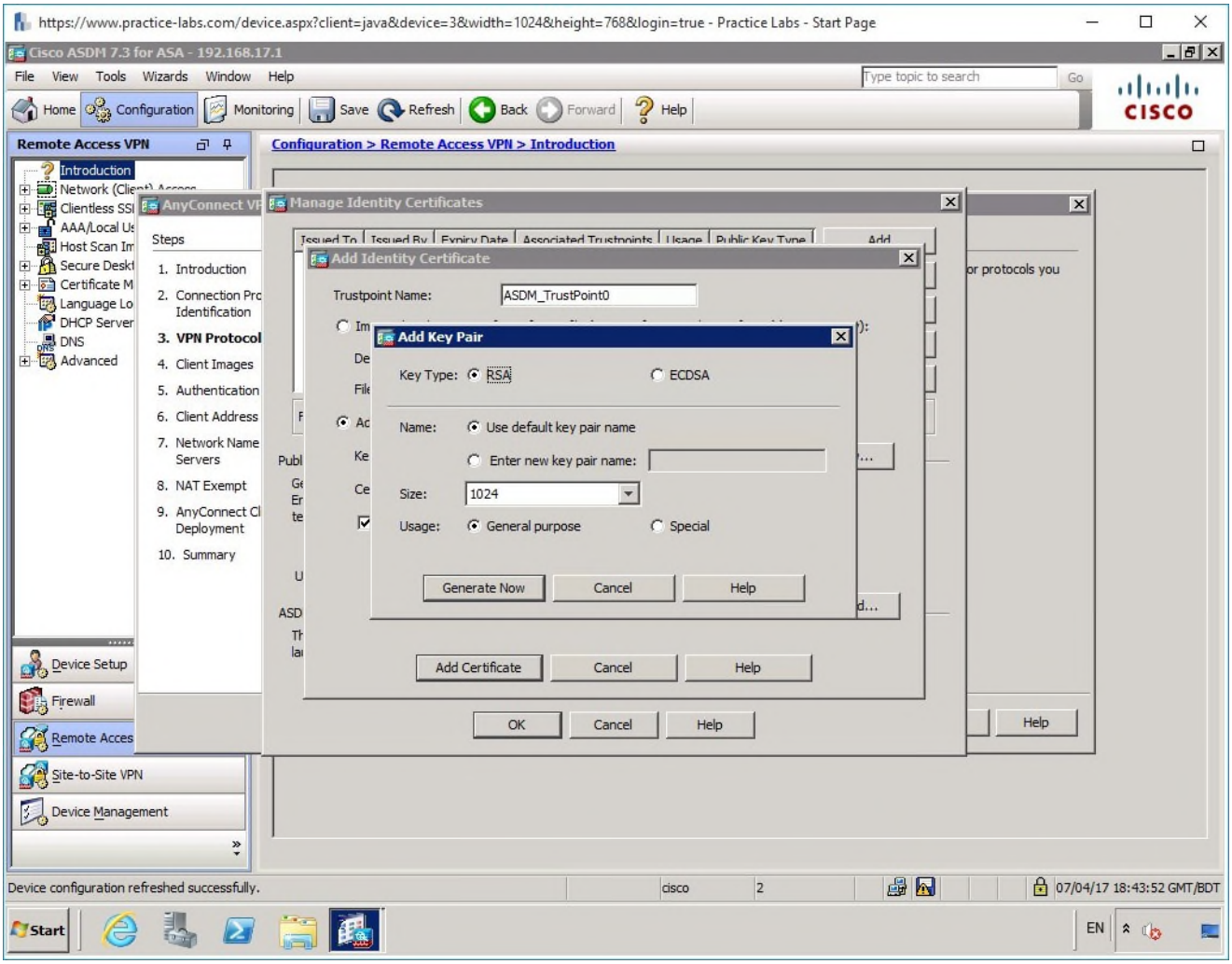


Figure 2.6 Screenshot of the Add Key Pair window: Notice the selection of values for the “Key Type”, “Name”, “Size”, and “Usage” fields.

Use the defaults for this example and click **Generate Now**, the page will go back to the previous dialog and populate the key pair for you.

Click **Add Certificate** (ensure **Add a new identity** is still selected):

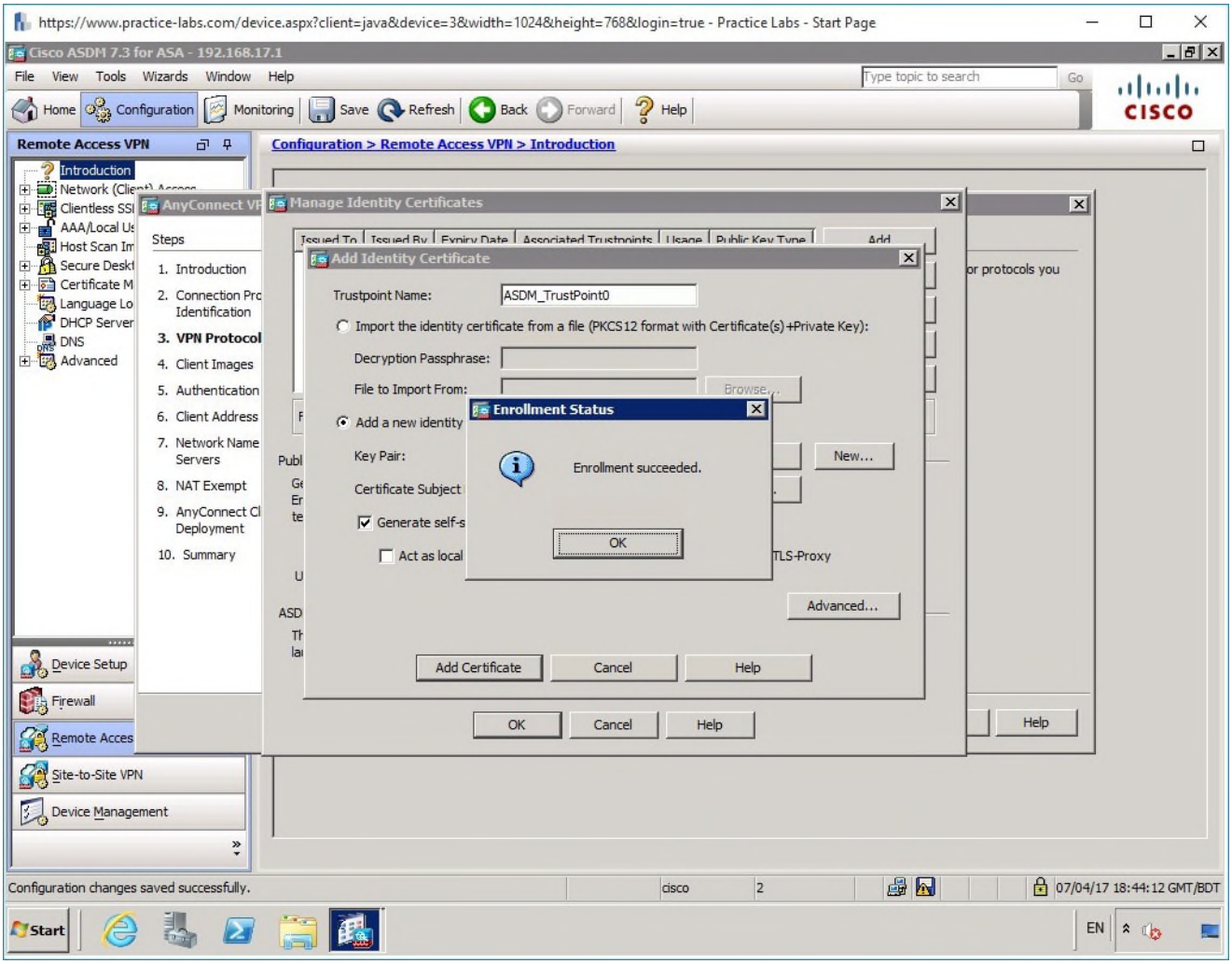


Figure 2.7 Screenshot of the Enrollment Status window: Notice the enrollment success message.

Click **OK**.

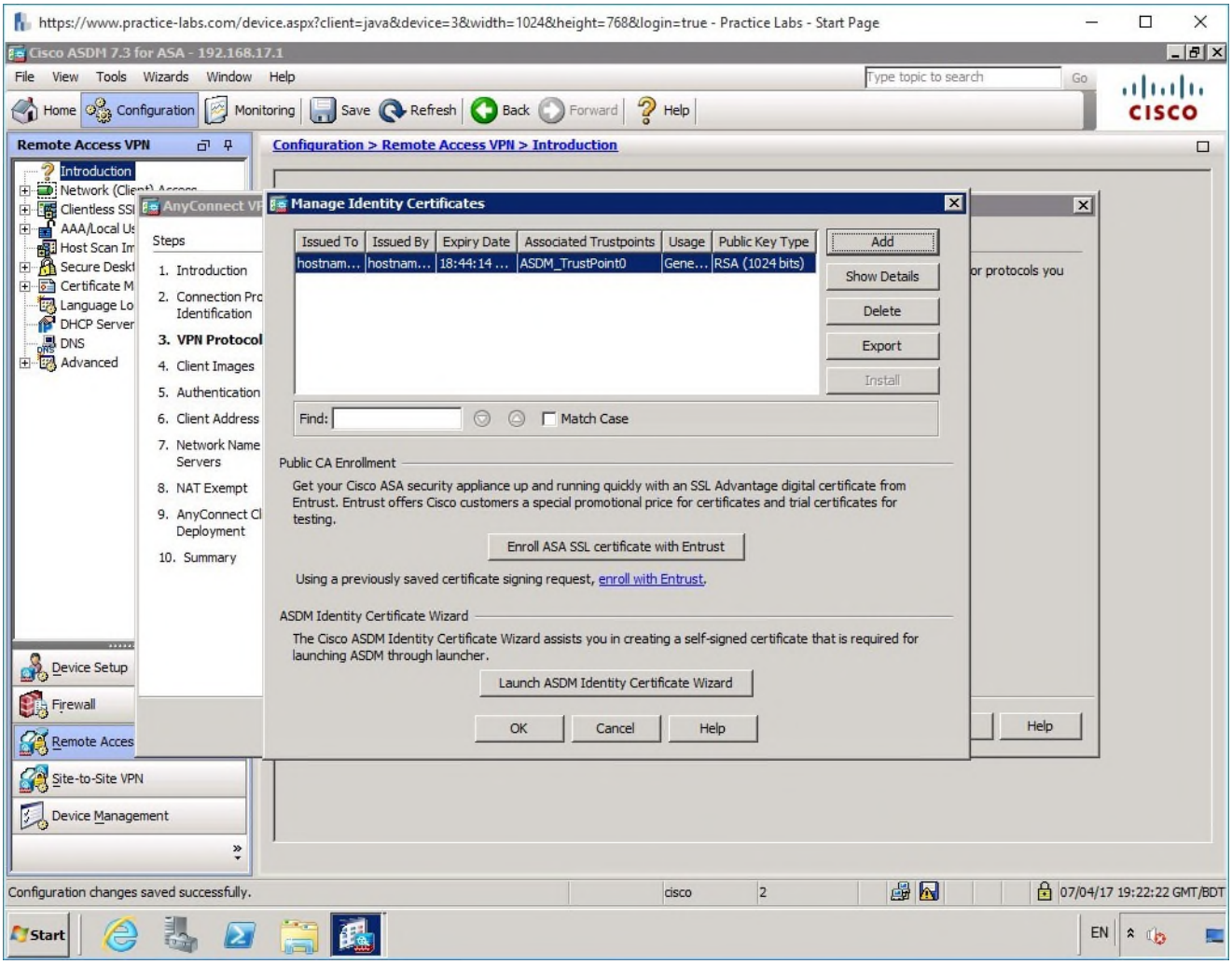


Figure 2.8 Screenshot of the Manage Identity Certificates window: Notice the addition of a host. The complete details of the host, such as hostname and issued by, are listed under various columns.

Click **OK** again, then click **Next** to continue the wizard.

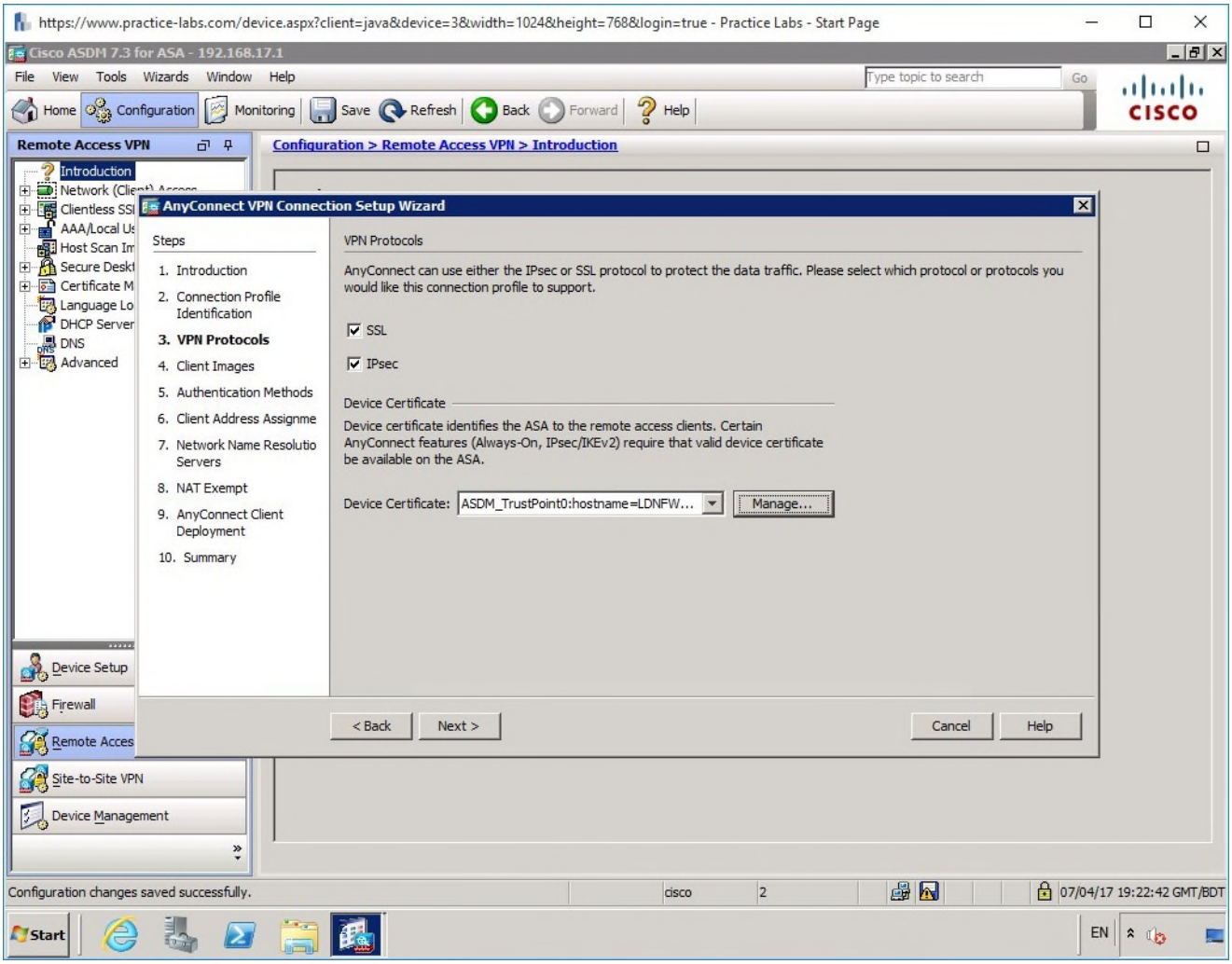


Figure 2.9 Screenshot of the AnyConnect VPN Connection Setup Wizard window: Notice the addition of device certificate in the “Device Certificate” field.

Step 5

On the **Client Images** page, click **Add**:

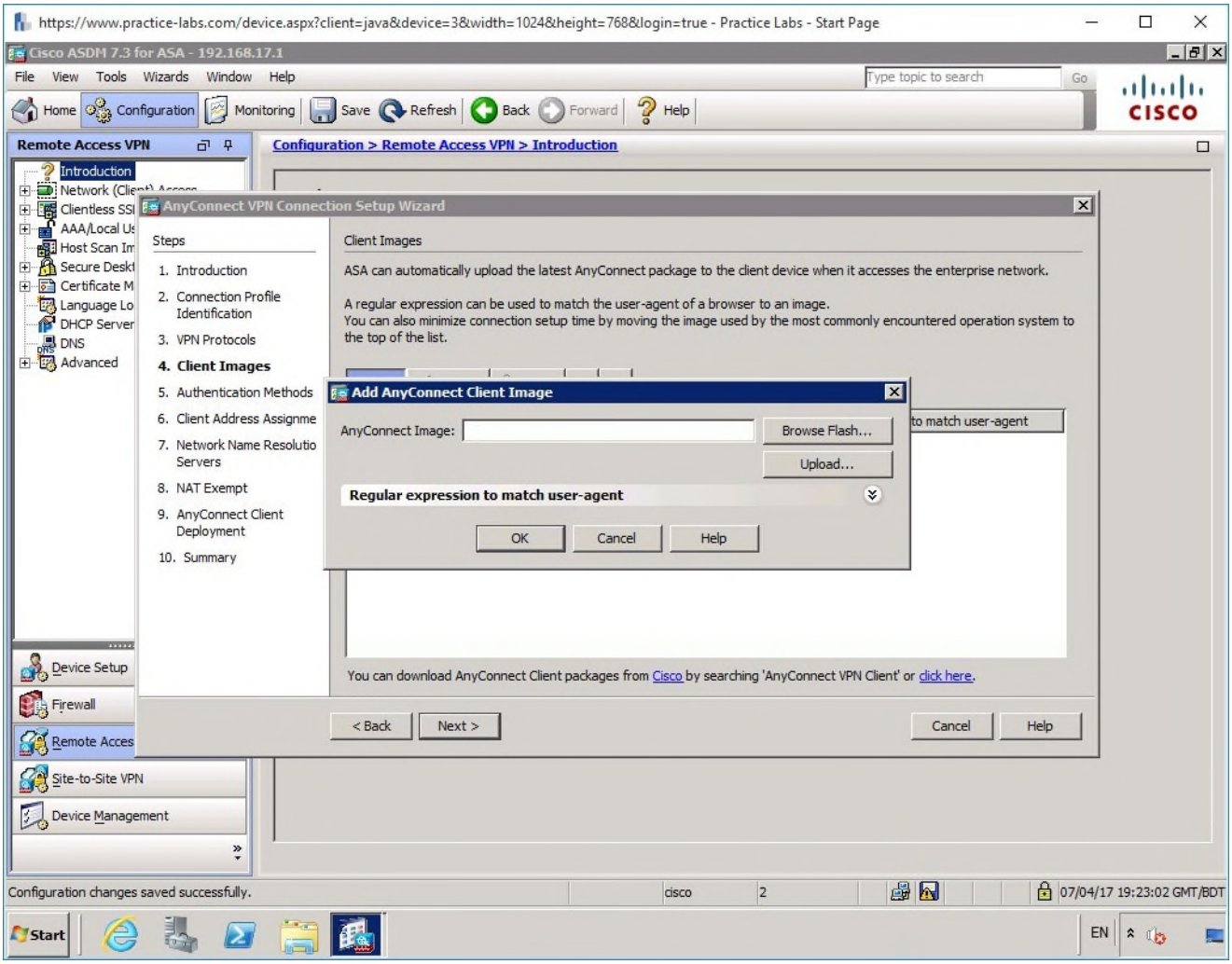


Figure 2.10 Screenshot of the initial “Add AnyConnect Client Image” window: User is prompted to add an AnyConnect Image.

Click **Browse flash** and select the latest version of the AnyConnect client on the flash, for example in the screenshot; the latest version is **anyconnect-win-3.1.05182-k9.pkg**

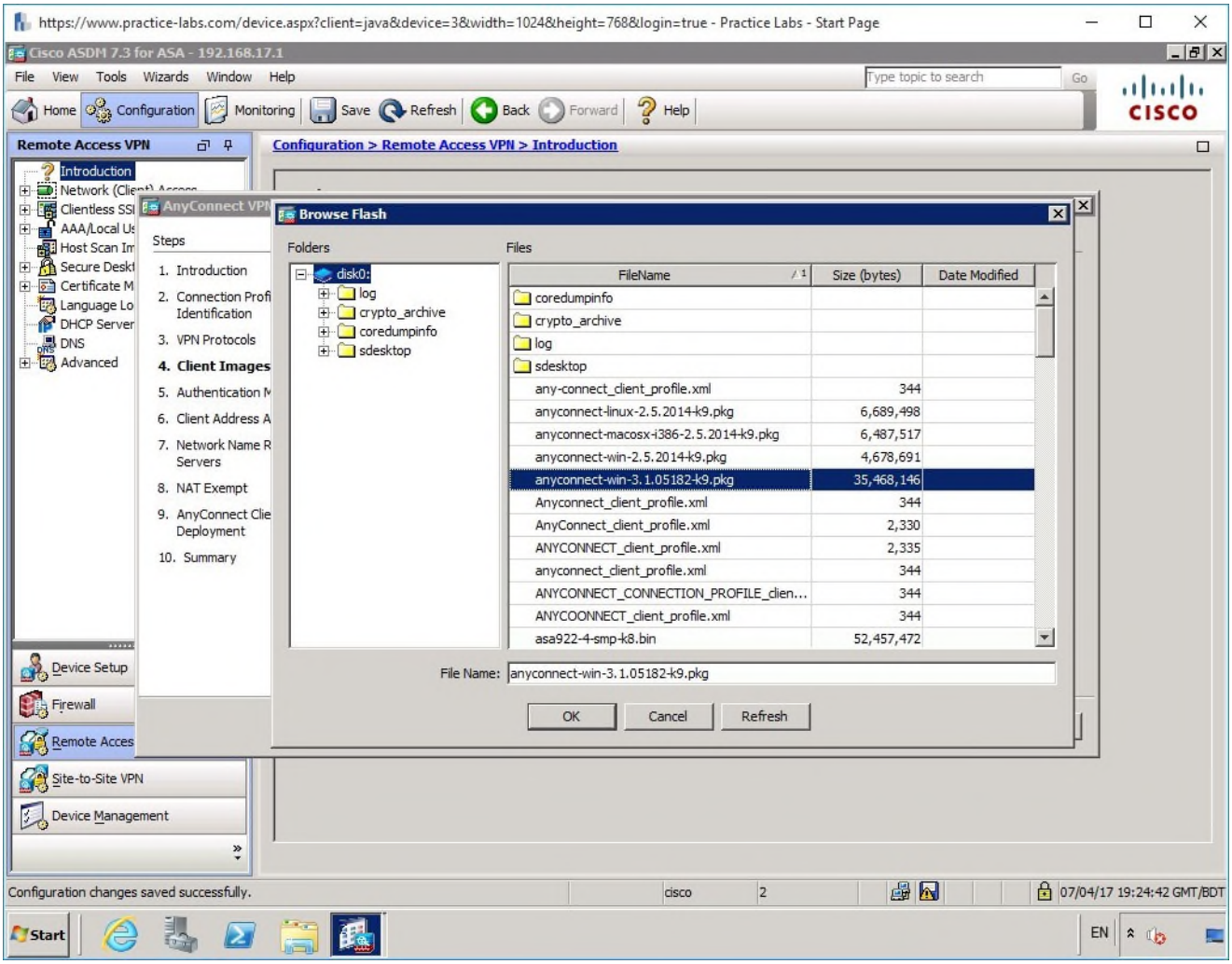


Figure 2.11 Screenshot of the Browse Flash window: User can select an AnyConnect Image to add.

Click **OK** once selected, then click **OK** again.

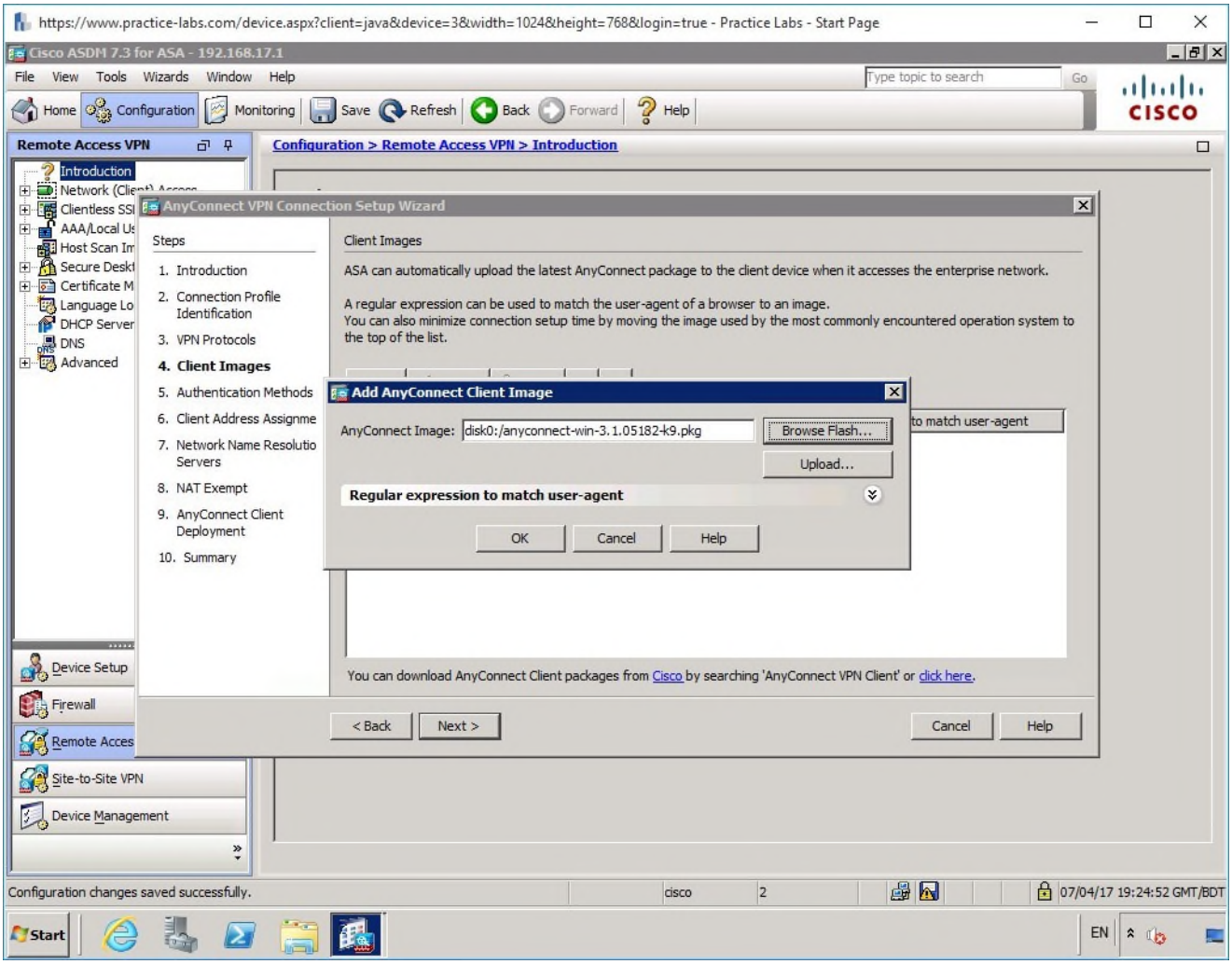


Figure 2.12 Screenshot of the Add AnyConnect Client Image window: Notice the path of the image added into the AnyConnect Image field.

> ***Note:*** *The AnyConnect client must be downloaded from the Cisco website with a relevant service contract.*

At the wizard, click **Next** to continue:

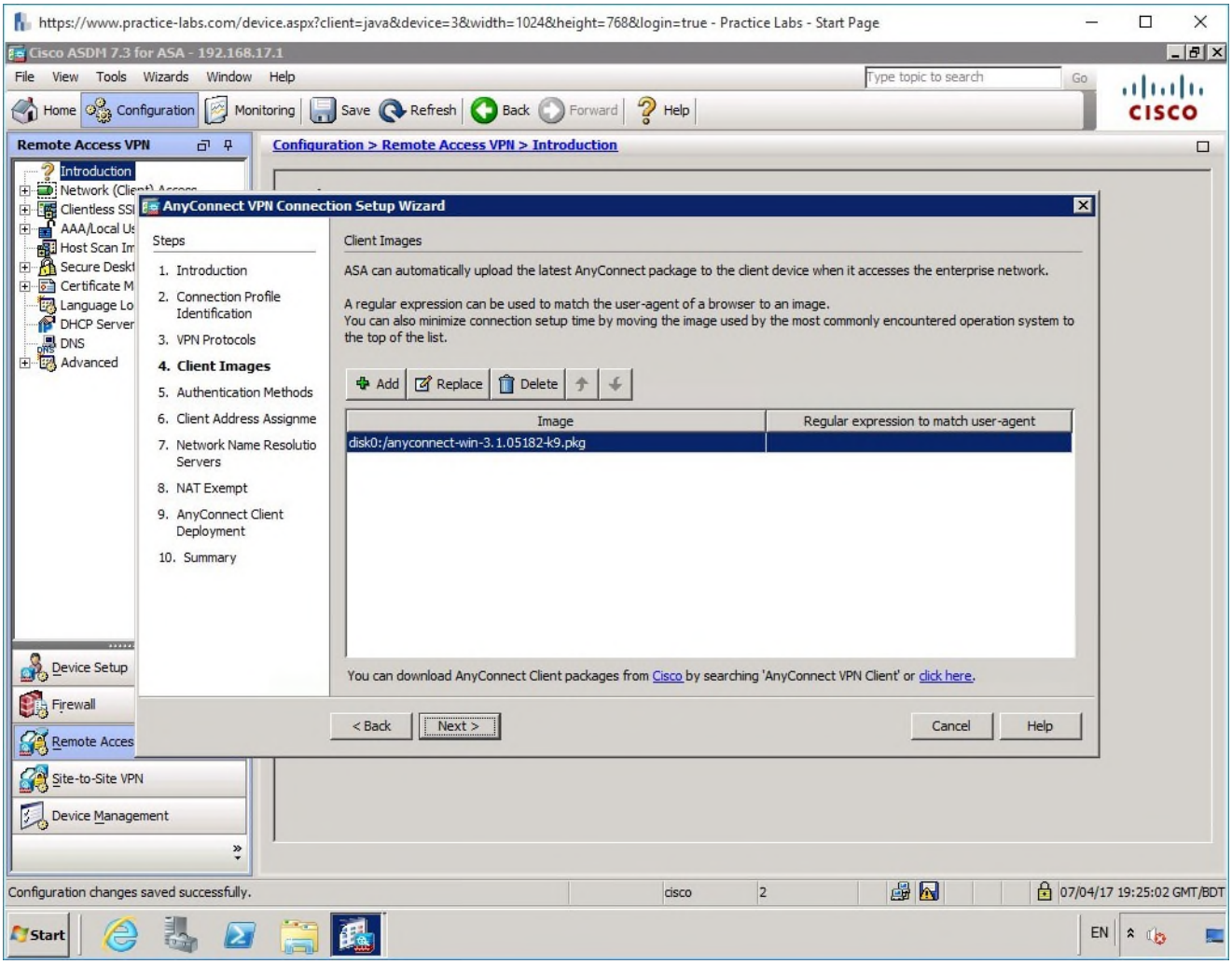


Figure 2.13 Screenshot of the Client Images page of the AnyConnect VPN Connection Setup Wizard window: Notice the path of the image added. Relevant details are displayed under the “Image” and “Regular expression to match user agent” columns.

Step 6

On the **User Authentication** page, ensure the AAA server group says **LOCAL**:

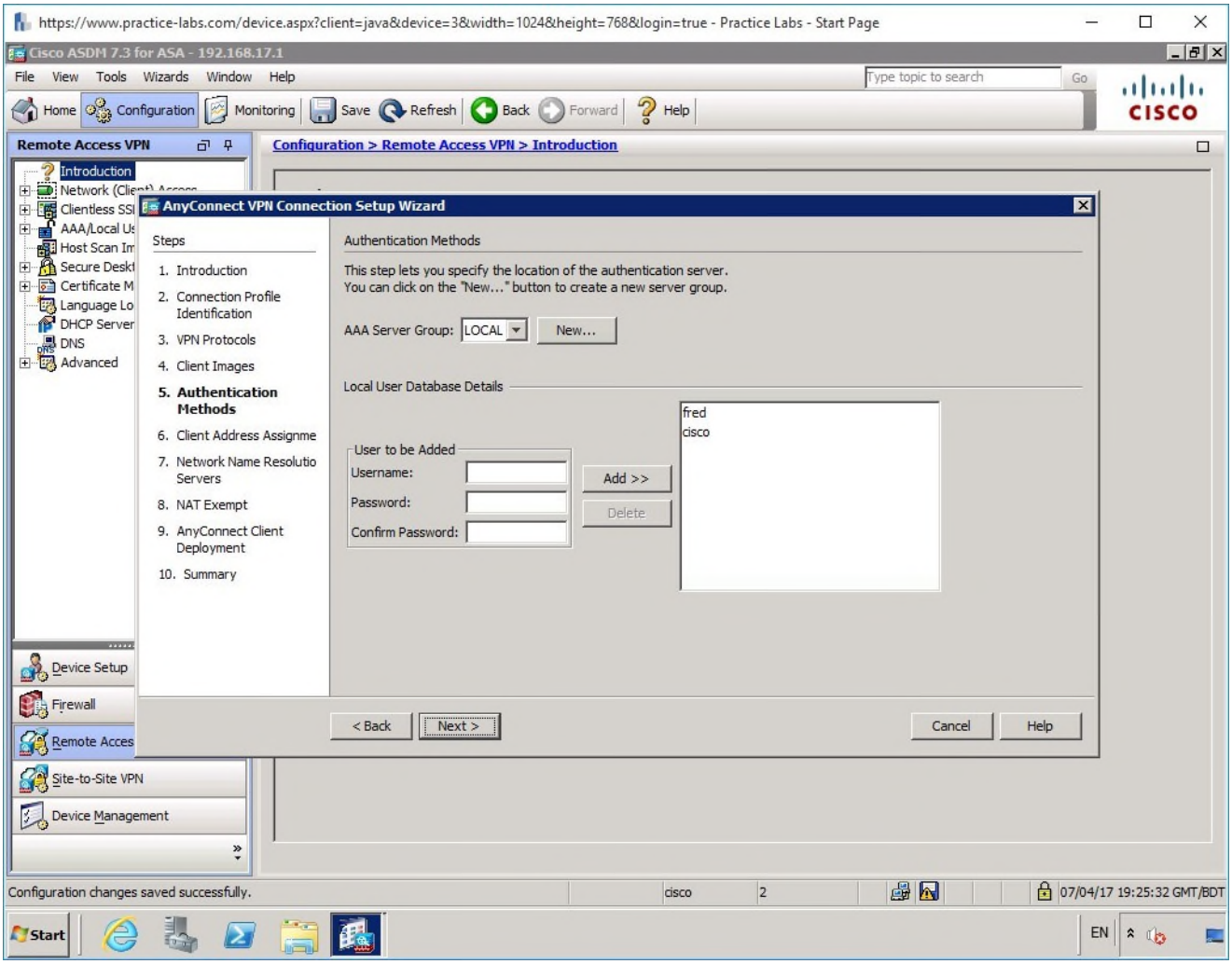


Figure 2.14 Screenshot of the Authentication Methods page of the AnyConnect VPN Connection Setup Wizard window: Notice the selection of LOCAL value in the "AAA Server Group" field.

As we already have a user created in the previous exercise we don't need to create any more accounts, click **Next**.

Step 7

On the address assignments page click **New** to create a new address pool:

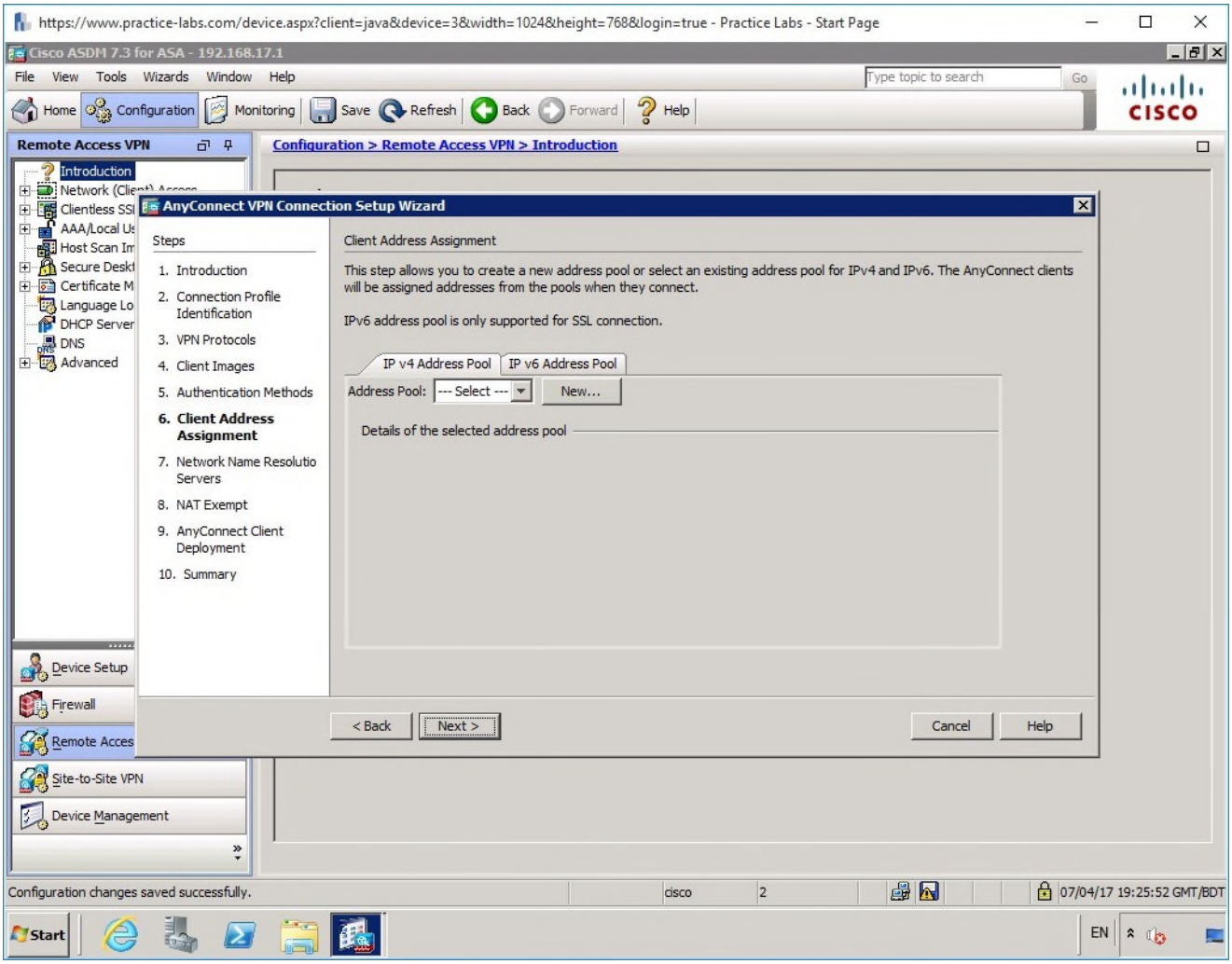


Figure 2.15 Screenshot of the initial screen of the Client Address Assignment page of the AnyConnect VPN Connection Setup Wizard window: User needs to add an address pool.

In the dialog window that appears, enter the following details:

- Name: **AnyConnect_POOL**
- Starting IP Address: **192.168.18.15**
- Ending IP Address: **192.168.18.254**
- Subnet Mask: **255.255.255.0**

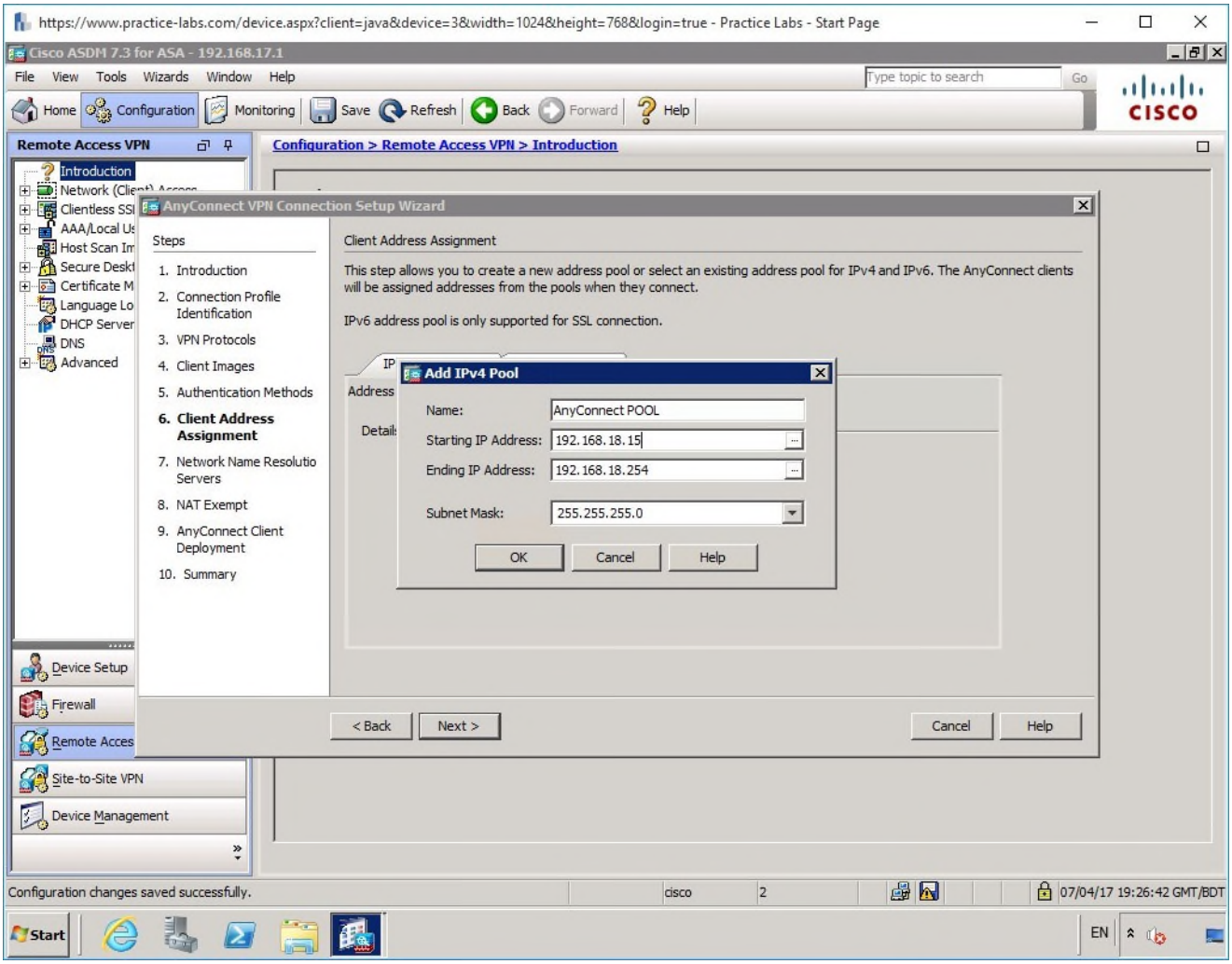


Figure 2.16 Screenshot of the Add IPv4 Pool window: User needs to create a new pool. Notice the values defines in various fields.

Click **OK** once you have entered in the pool information. Then at the wizard prompt, click **Next** to continue.

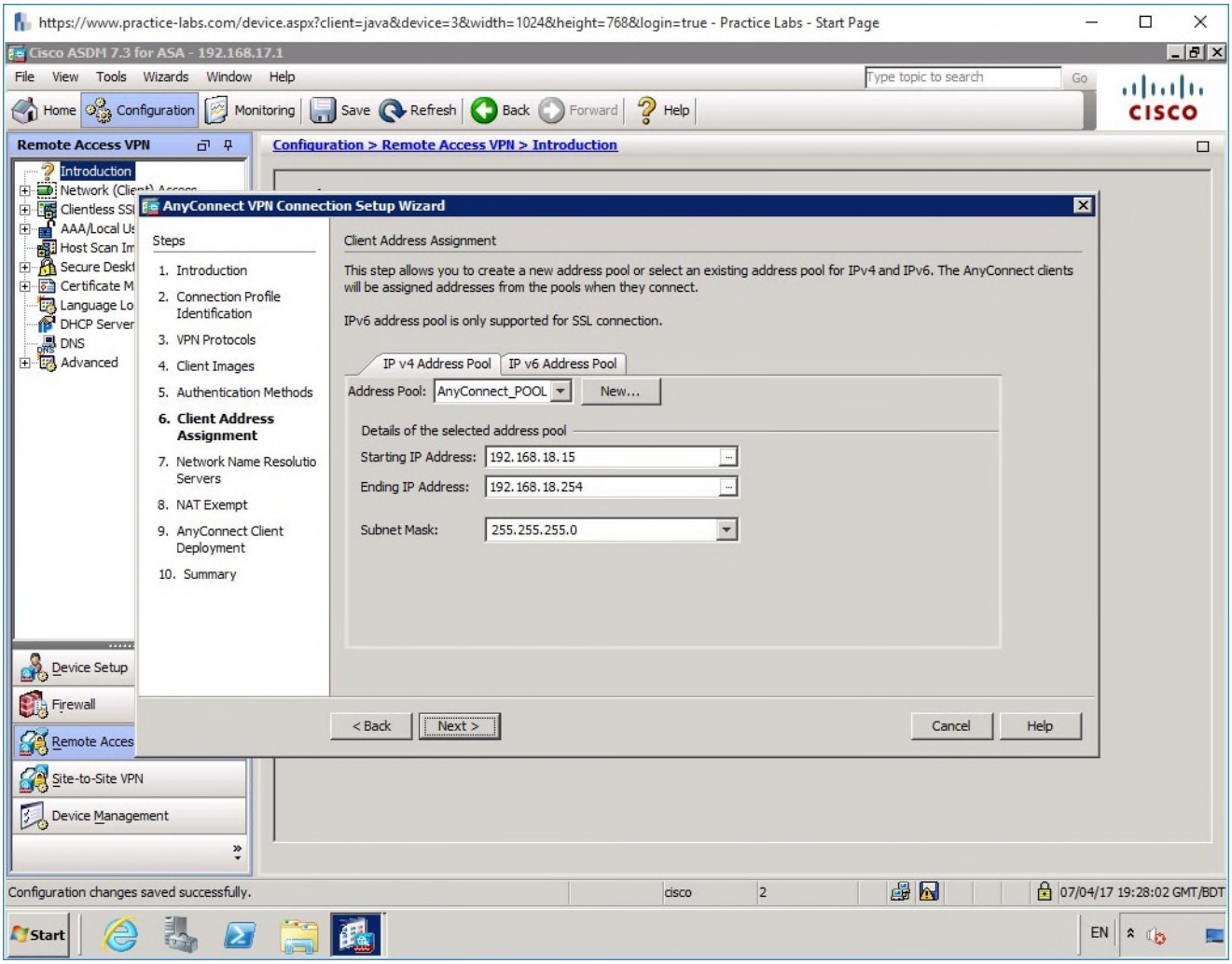


Figure 2.17 Screenshot of the filled Client Address Assignment page of the AnyConnect VPN Connection Setup Wizard window: Notice the defined IP address range.

Step 8

On the DNS / WINS page, use the following settings:

- DNS Servers: **192.168.16.10**
- WINS Servers: **192.168.16.10**
- Domain Name: **practice-labs.com**

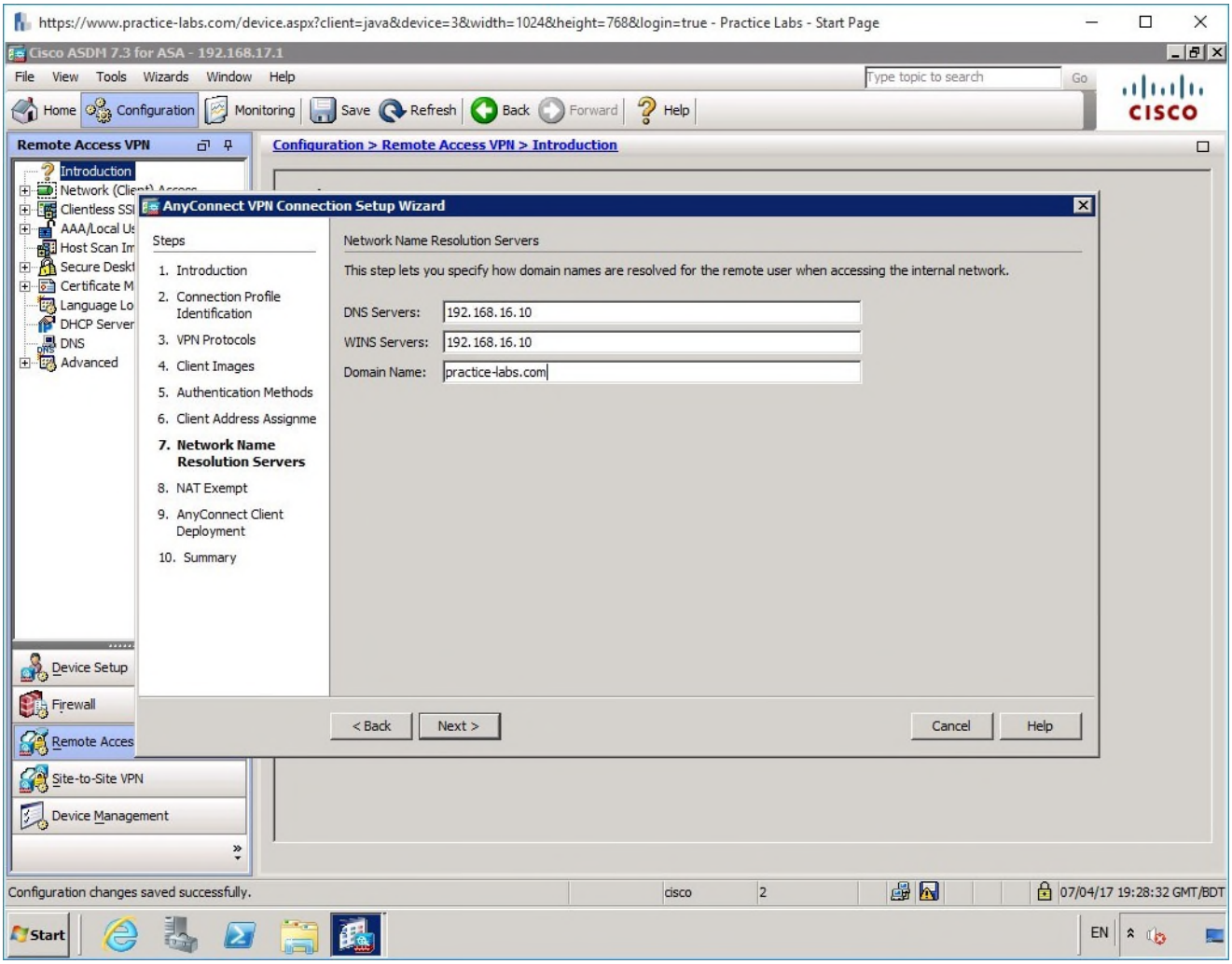


Figure 2.18 Screenshot of the Network Name Resolution Servers page of the AnyConnect VPN Connection Setup Wizard window: User needs to add the appropriate values in the “DNS Servers”, “WINS Servers”, and “Domain Name” fields.

> ***Note:*** *192.168.16.10 is not a DNS or WINS server. However, it's not necessary for this task.*

Click **Next**.

Step 9

On the NAT Exempt page, we want to exclude our inside network, check the **Exempt VPN traffic from network address translation** checkbox, ensure the **Inside** interface is selected correctly.

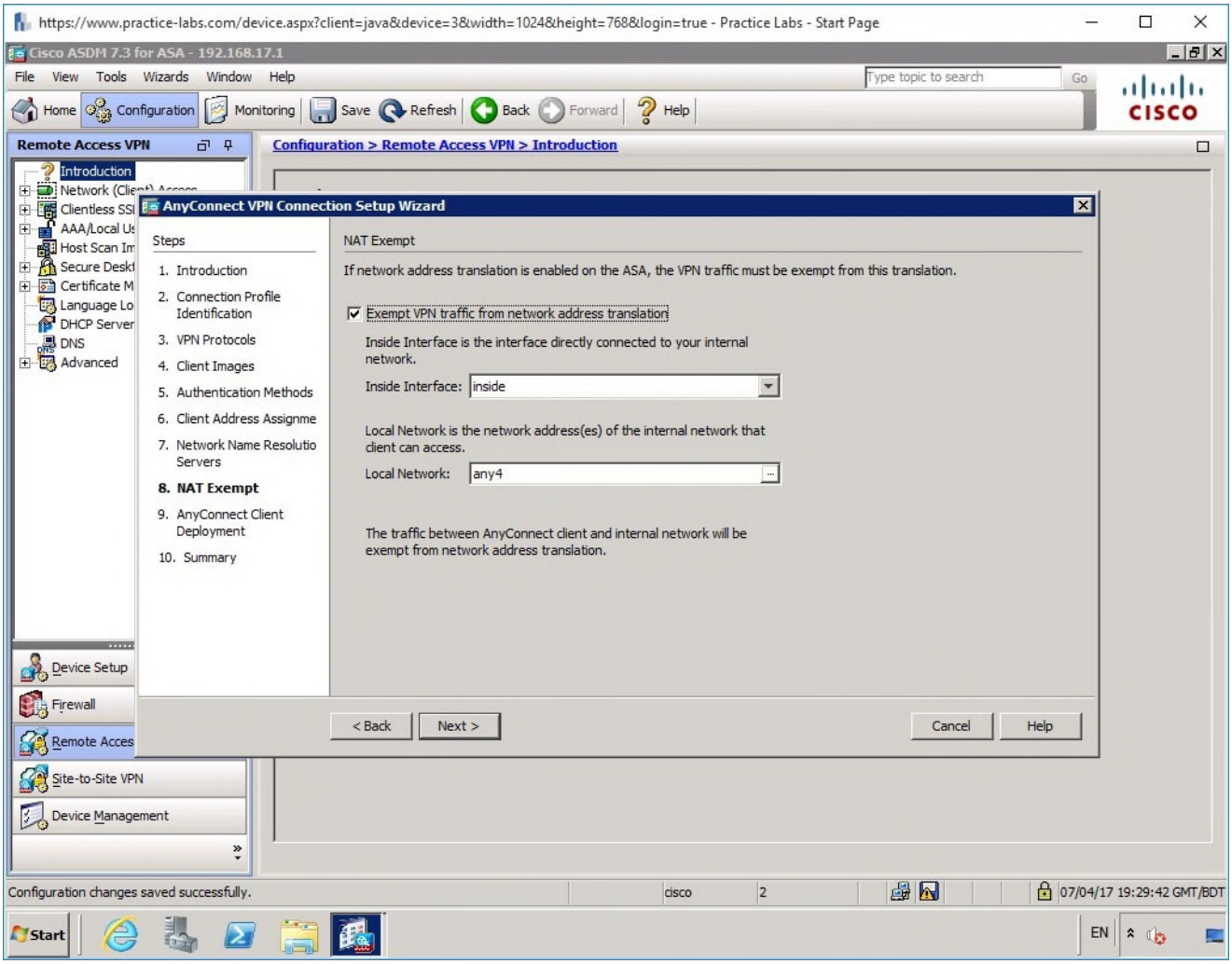


Figure 2.19 Screenshot of the NAT Exempt page of the AnyConnect VPN Connection Setup Wizard window: User needs select the Exempt VPN traffic from network address translation. Notice the Inside is selected in the "Inside Interface" field and any4 is selected for "Local Network" field.

In the Local Network, click the ellipses button to select the correct internal address space:

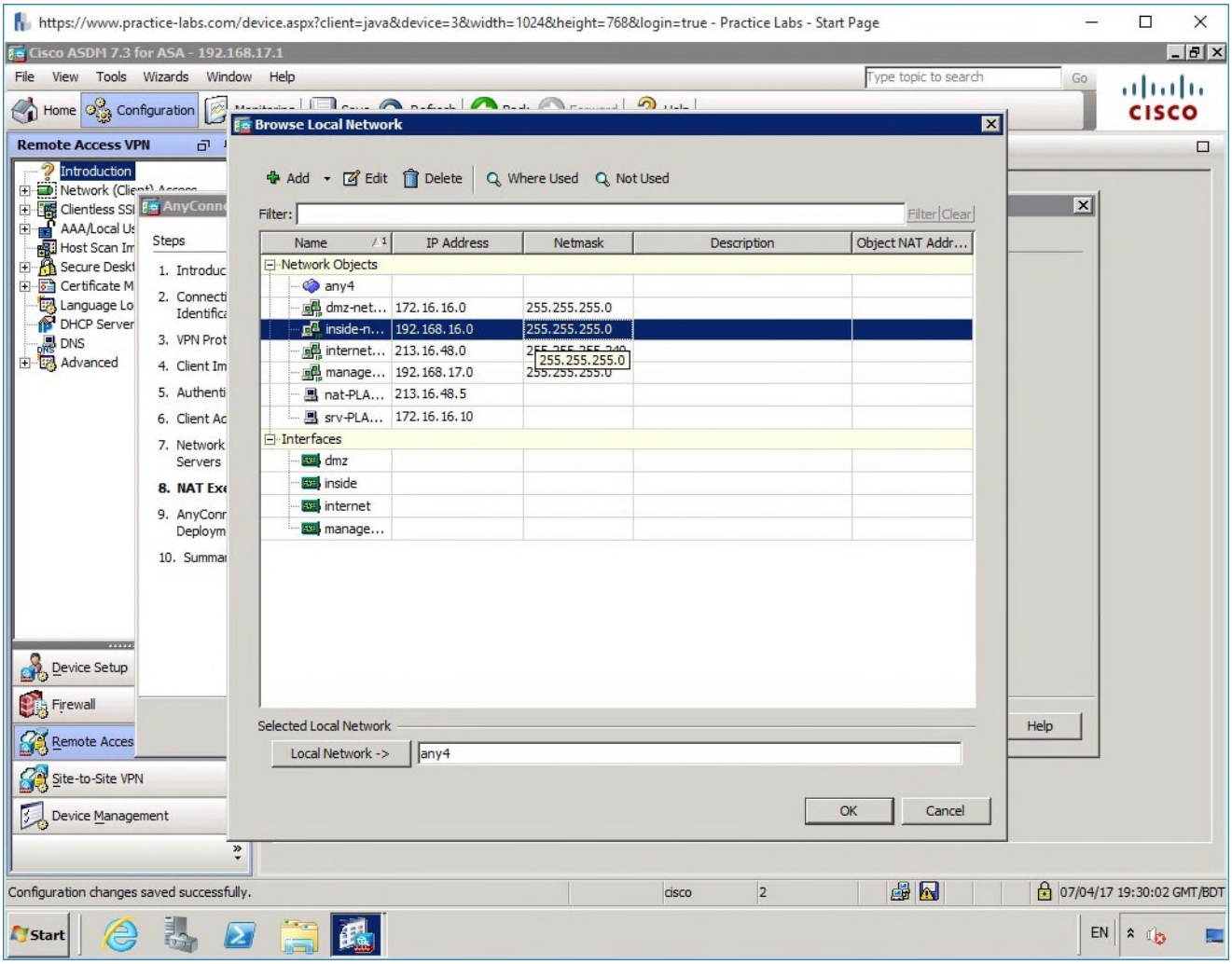


Figure 2.20 Screenshot of Browse Local Network window: User needs select an internal address space.

Alert: Please ensure that the **inside-network/24** is inside of the **Local Network ->** text box.

Once you have selected the 192.168.16.0/24 subnet click **OK**.

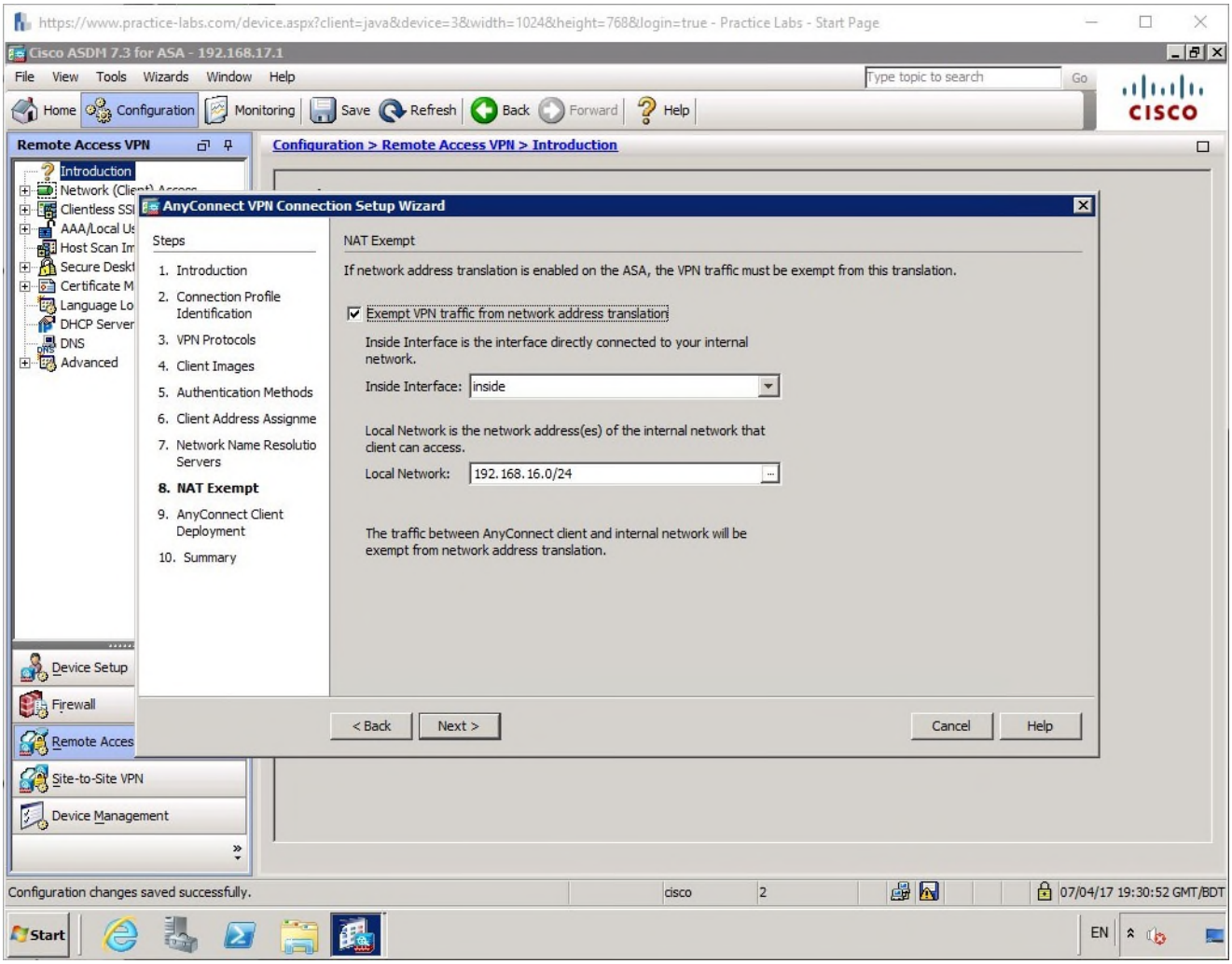


Figure 2.21 Screenshot of the NAT Exempt page of the AnyConnect VPN Connection Setup Wizard window: Notice that the values in the "Local Network" field are updated with the selection of internal address space.

Click **Next** at the wizard.

Step 10

At the AnyConnect client deployment page, leave the defaults and allow web launch. Bear in mind you may want to modify this in your production environment and only deploy the client manually.

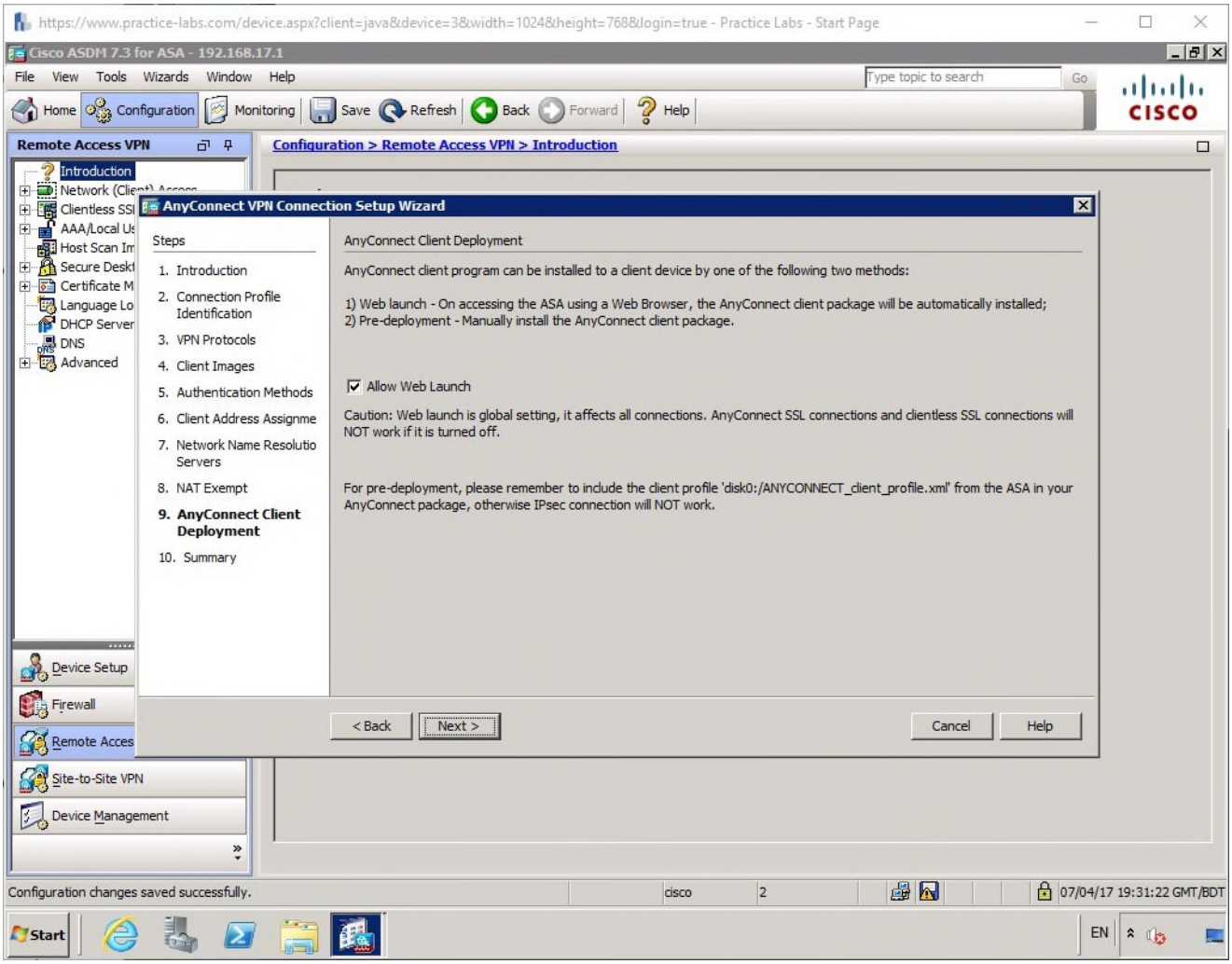


Figure 2.22 Screenshot of the AnyConnect Client Deployment page of the AnyConnect VPN Connection Setup Wizard window: Notice the selection of "Allow Web Launch" field as the default configuration.

Click **Next**.

Step 11

Finally, click **Finish** to deploy the configuration.

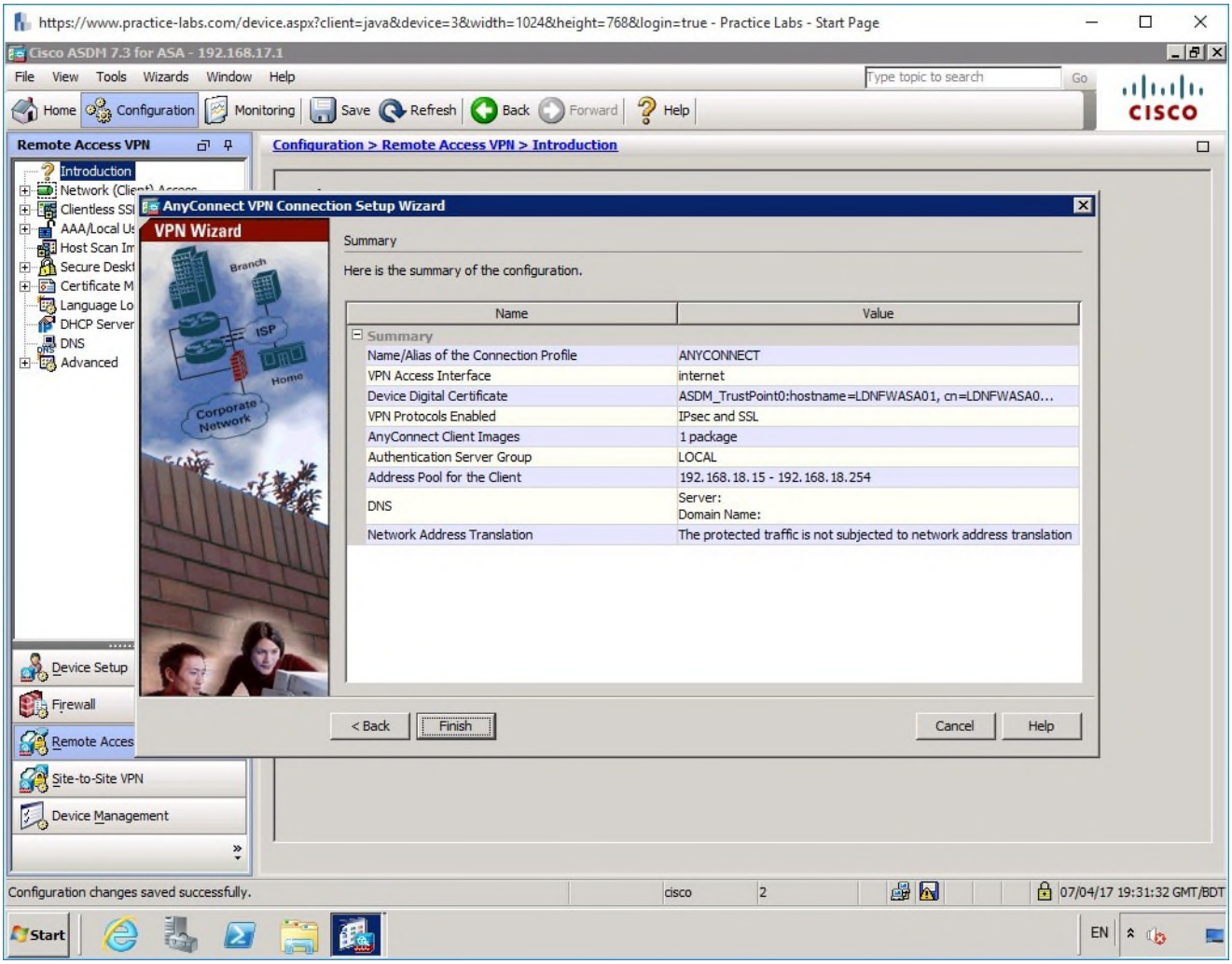


Figure 2.23 Screenshot of the Summary page of the AnyConnect VPN Connection Setup Wizard window: User needs to review the configuration before finalizing it.

Step 12

In the left panel of the ASDM software, ensure Remote Access VPN is selected, then expand Network (Client) Access the click **group Policies**.

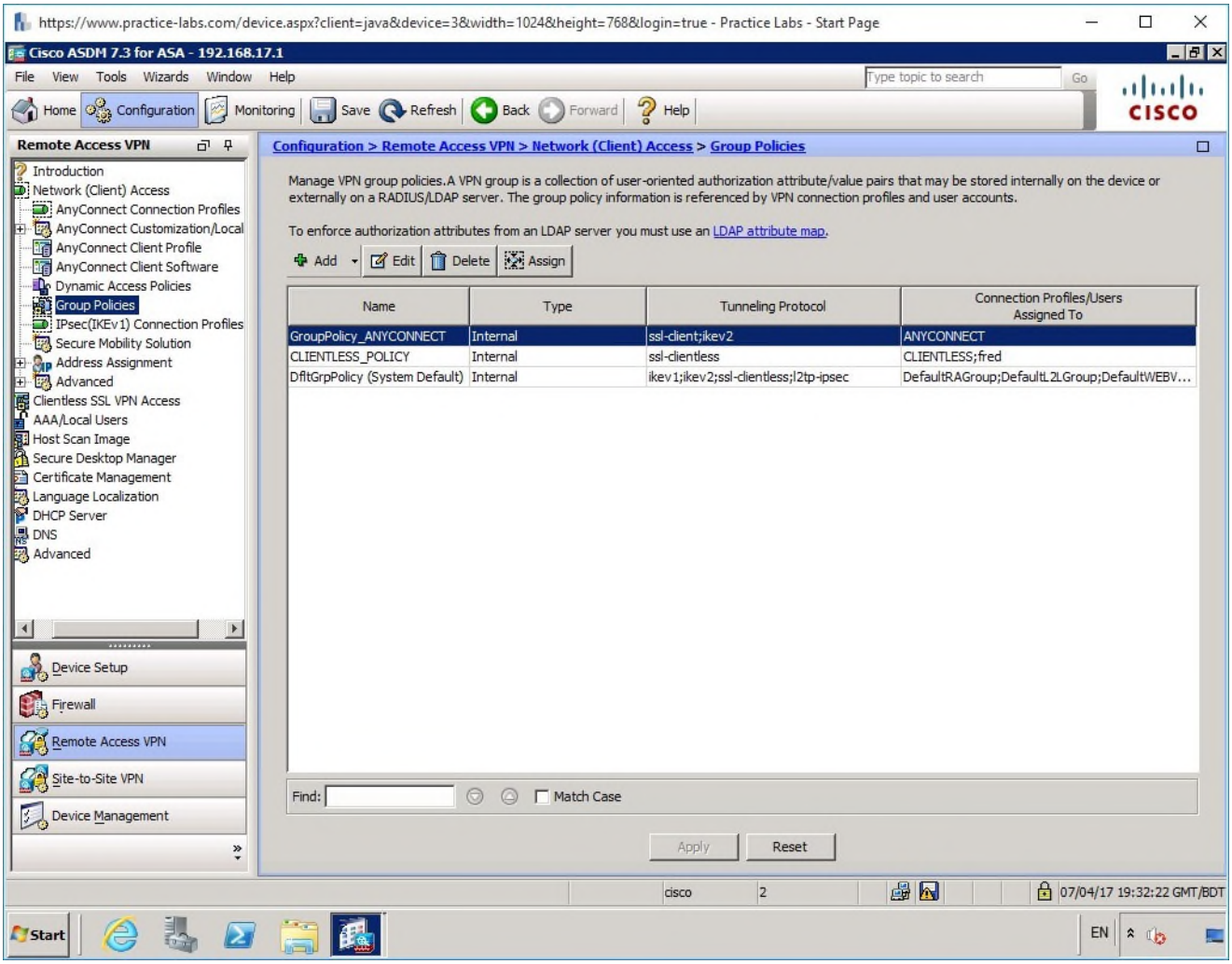


Figure 2.24 Screenshot of the Group Policies page of the AnyConnect VPN Connection Setup Wizard window: Notice the availability of different Group Policies. User needs to select an appropriate Group Policy to proceed.

Select the **GroupPolicy_ANYCONNECT** and click **Assign** at the above this window.

Ensure **fred** is assigned this policy:

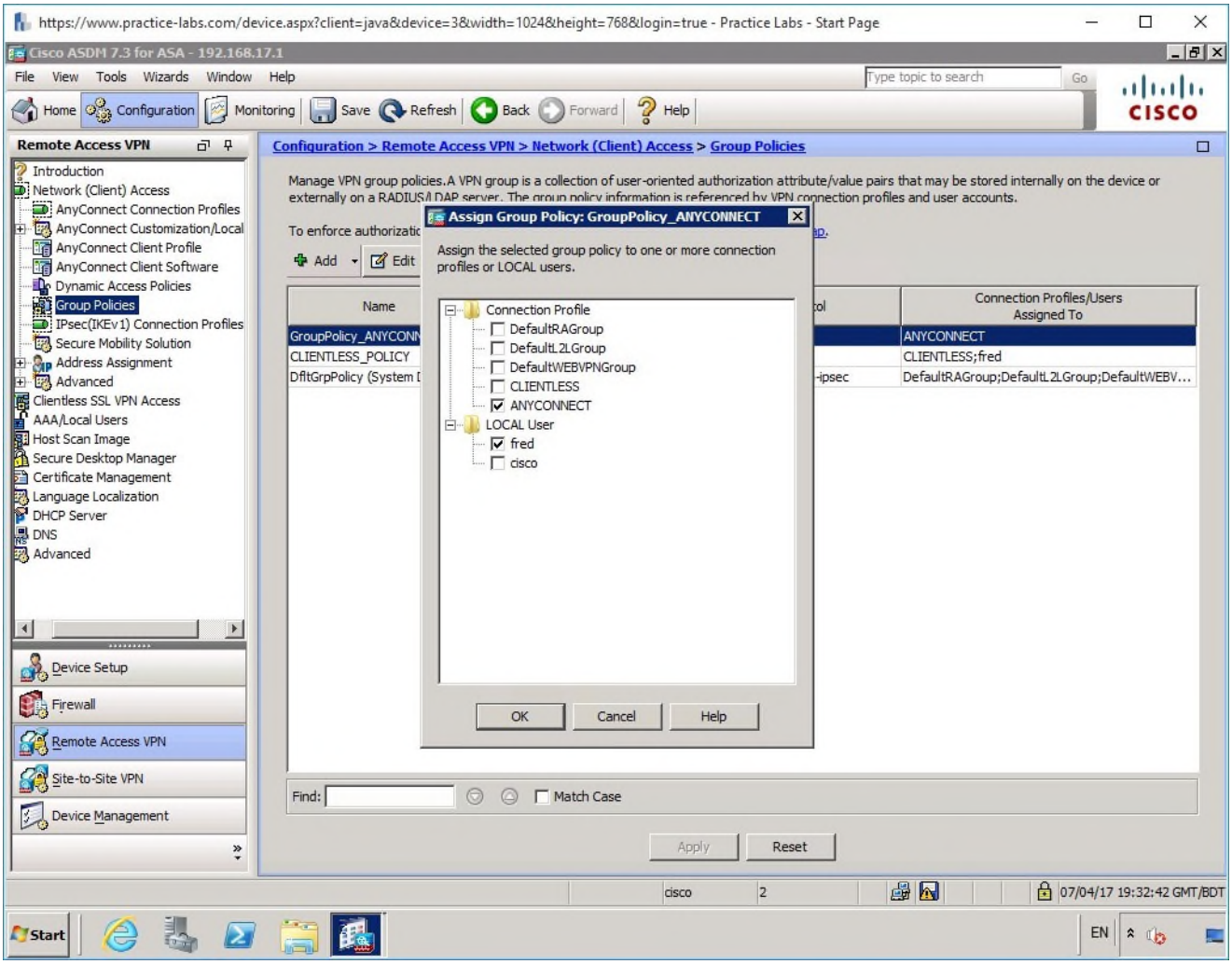


Figure 2.25 Screenshot of the Assign Group Policy: GroupPolicy_ANYCONNECT window. Notice the availability of different Group Policies. User needs to select an appropriate Group Policy to proceed.

Remember to click **Apply**.

Step 13

Next, go to PLABEXTCLI, if your Clientless SSL VPN connection is still active and hasn't timed out, click the **Logout** button. Then re-navigate to **https://213.16.48.1** ensure the ANYCONNECT profile is selected and login using **fred / cisco123**

Once you login you will receive this page:

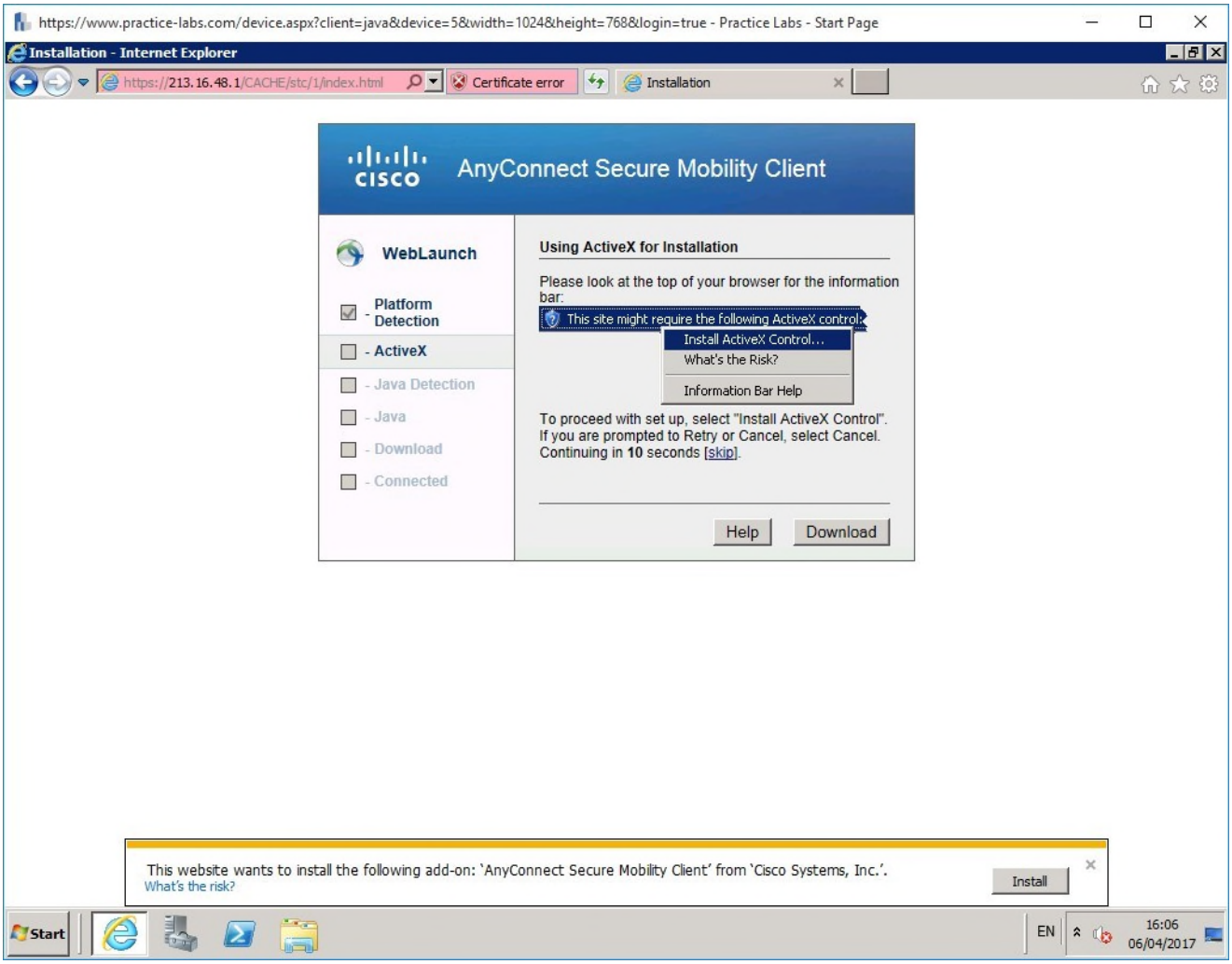


Figure 2.26 Screenshot of the post login window: User needs to download and install ActiveX control.

Click **OK** to the Java prompt and click **Install** at the bottom of the page:

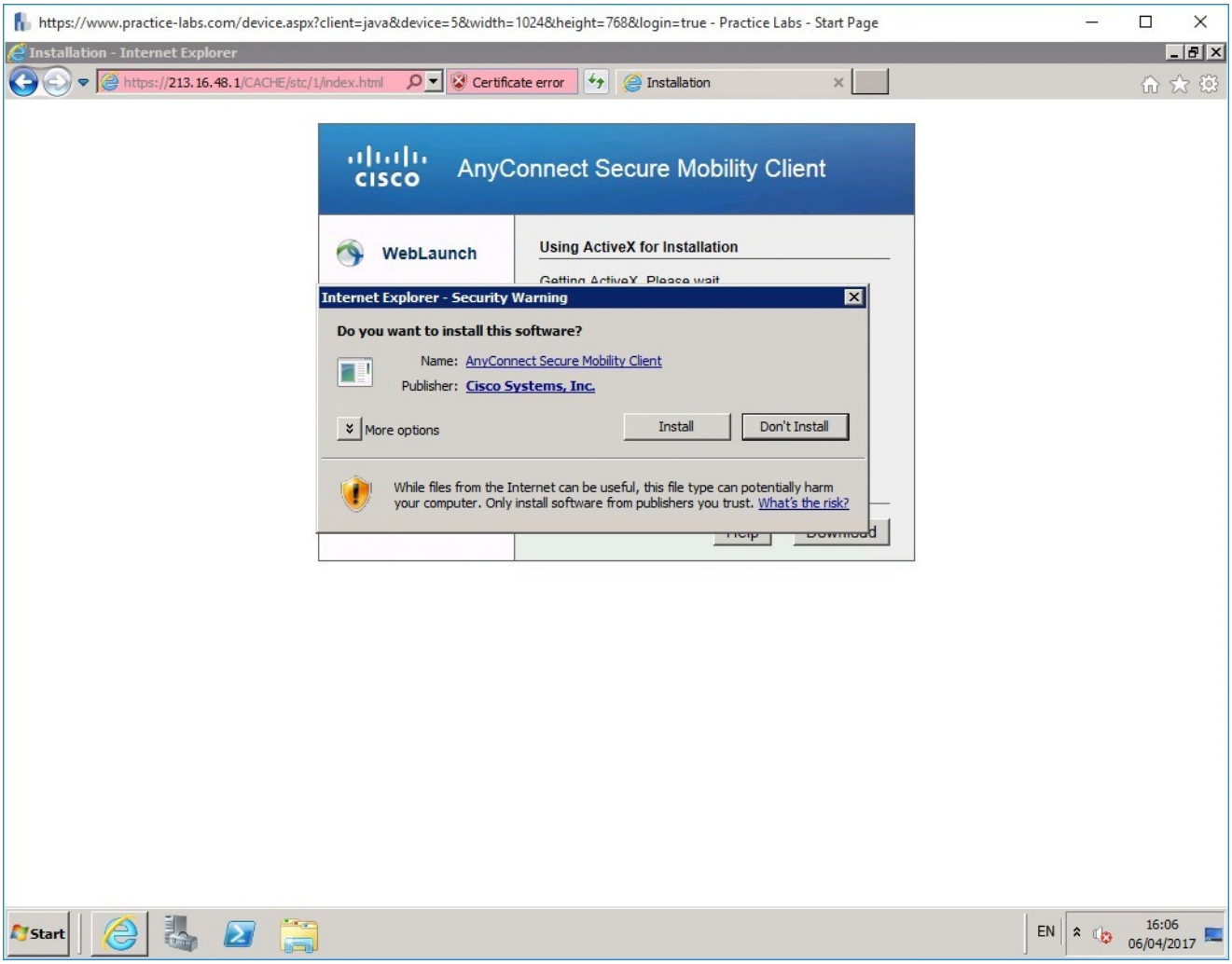


Figure 2.27 Screenshot of the Internet Explorer - Security Warning window: User needs to initiate the installation.

Click **Install** at the new dialog.

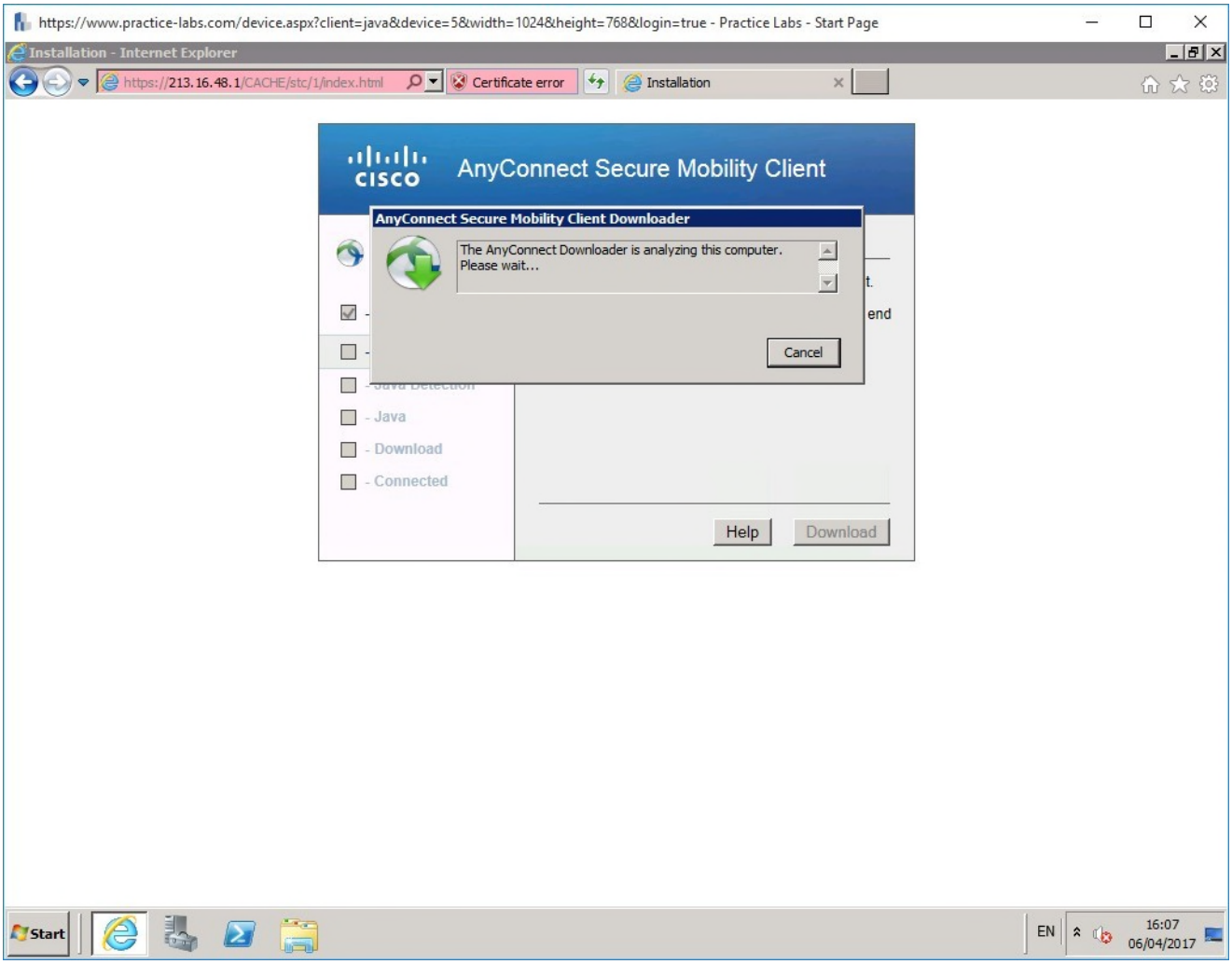


Figure 2.28 Screenshot of the AnyConnect Secure Mobility Client Downloader window: Notice that the downloader analyses the computer.

You will receive a warning saying the untrusted VPN server has been blocked:

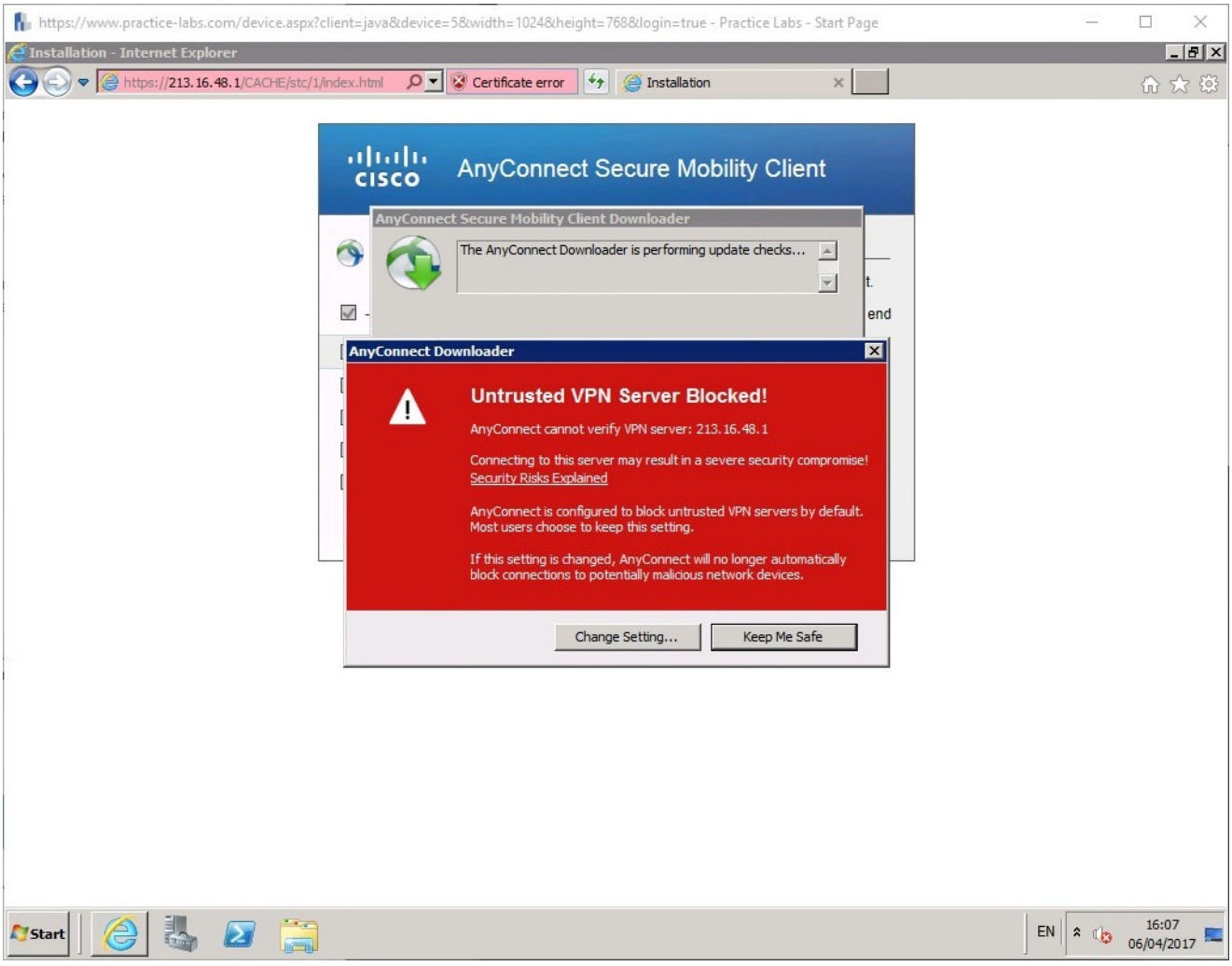


Figure 2.29 Screenshot of the AnyConnect Downloader window: Notice that the untrusted VPN Server is blocked.

Click the **Change Setting** button, then click **Apply Change.**

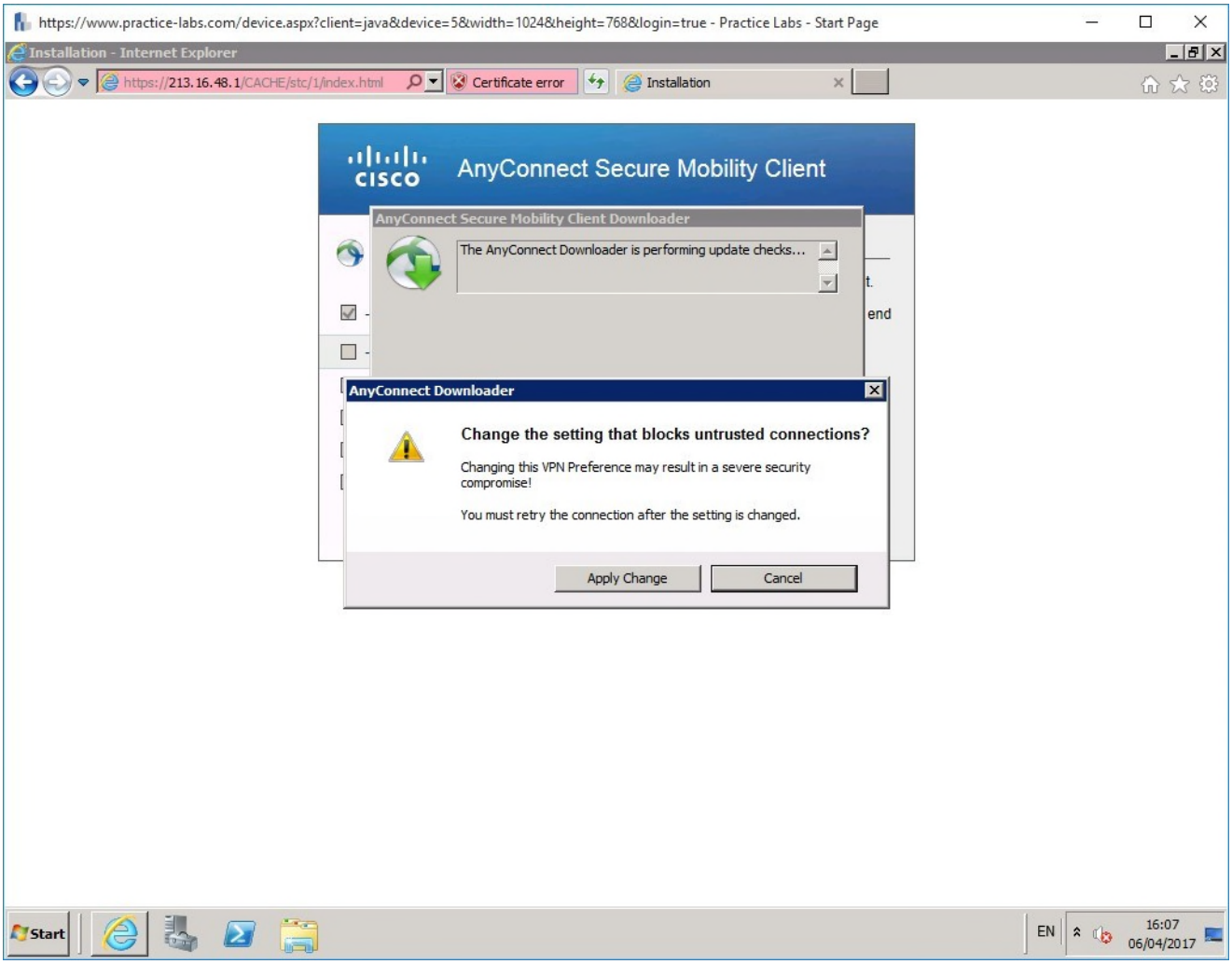


Figure 2.30 Screenshot of the AnyConnect Downloader window: User can change the settings to allow the blocked connections.

You now have to click the link on the page **retry the connection**:

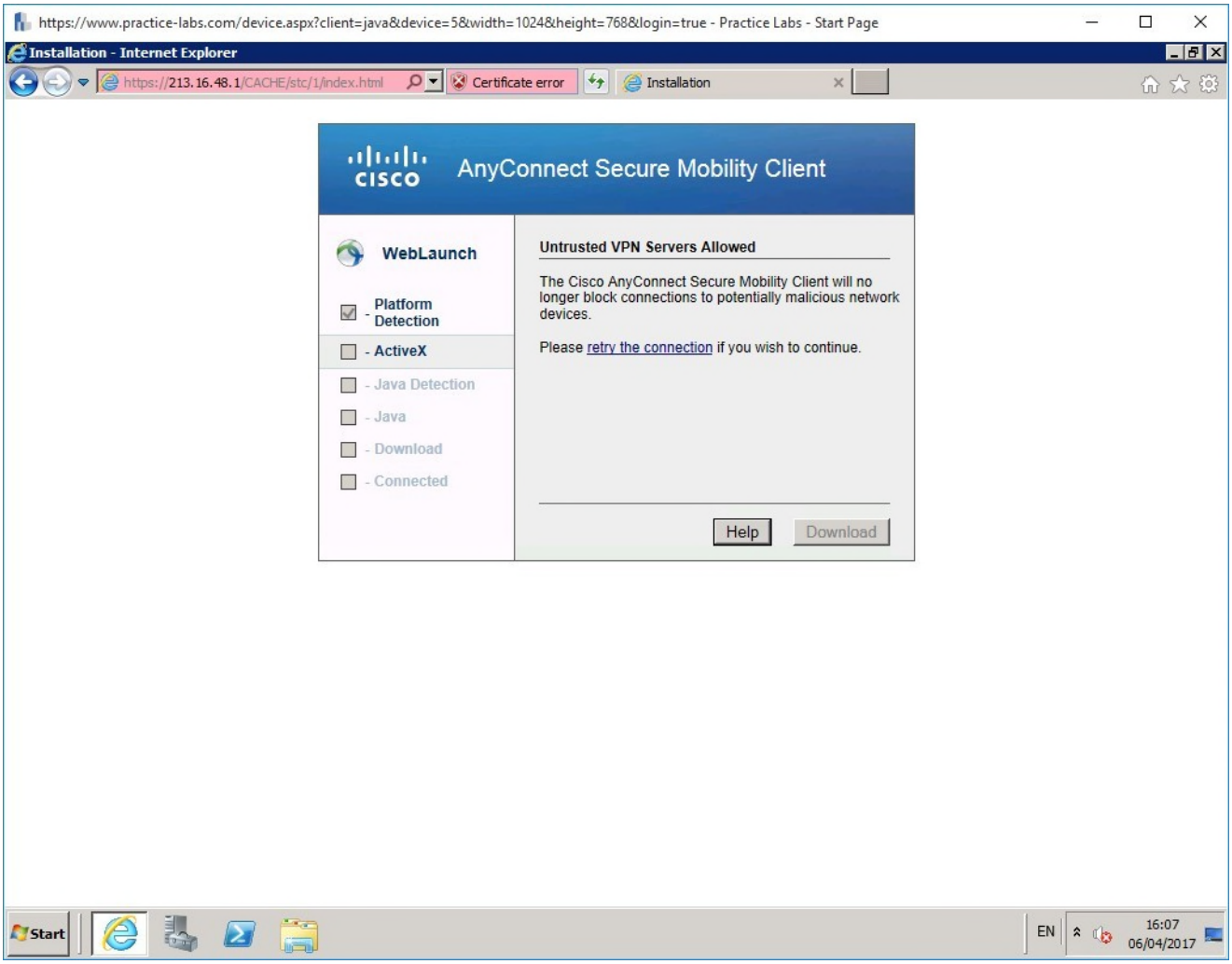


Figure 2.31 Screenshot of the AnyConnect Secure Mobility Client window: Notice that the untrusted VPN Servers are now allowed.

The process will restart again.

This time, you will get a security warning, now you can click **Connect Anyway**:

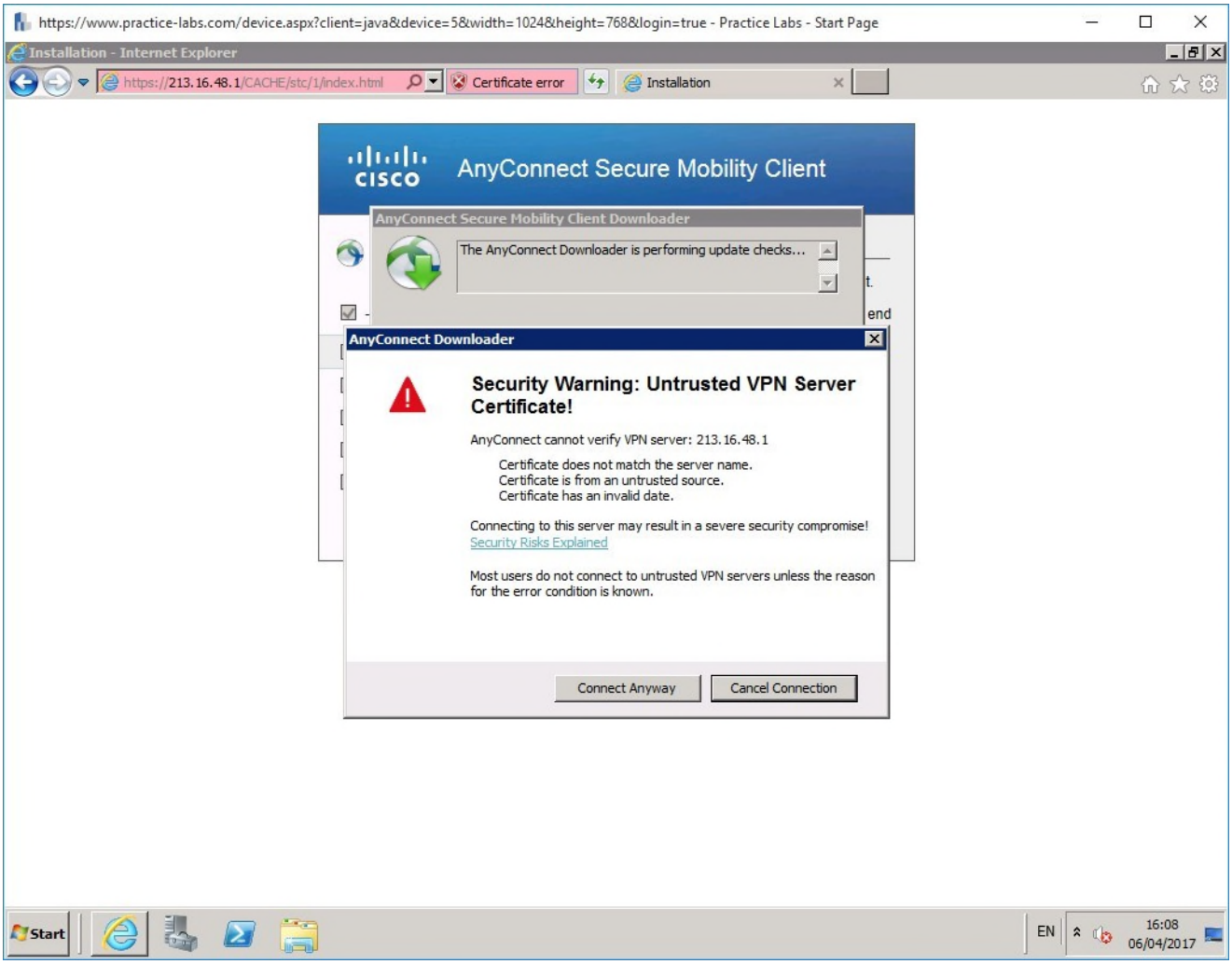


Figure 2.32 Screenshot of the AnyConnect Downloader window: Notice that this window displays the security warning about connecting with an untrusted VPN Server. It also notifies of the IP address of the untrusted VPN server.

The client will start to install.

Step 14

In the bottom system tray you will notice a new icon appear (this will disappear but is still running) for the AnyConnect client:

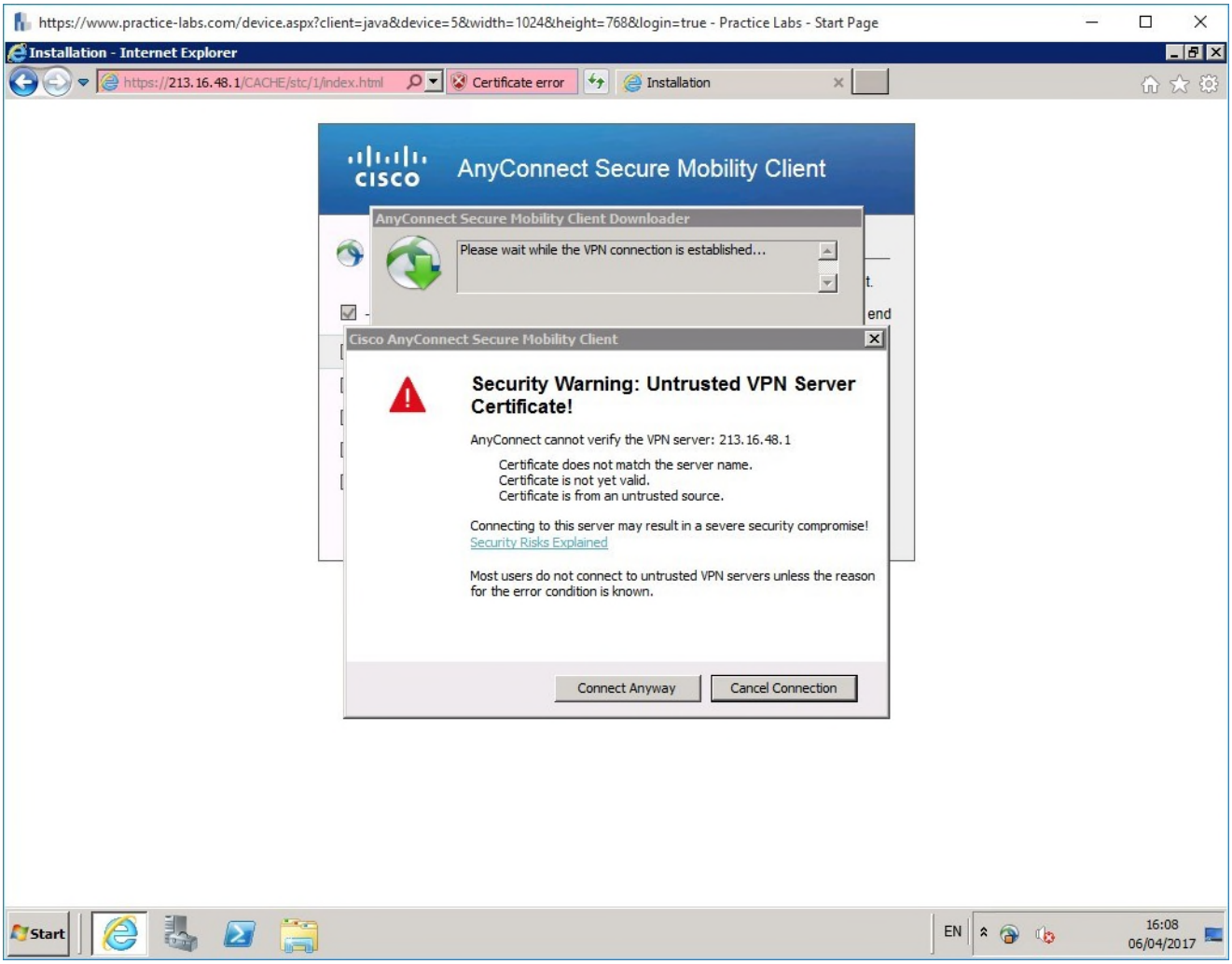


Figure 2.33 Screenshot of the Cisco AnyConnect Secure Mobility Client connection window: Notice after user acceptance to proceed, the Cisco AnyConnect Secure Mobility Client attempts to connect.

It looks like a small globe.

Click the **Connect Anyway** button again. An error will appear:

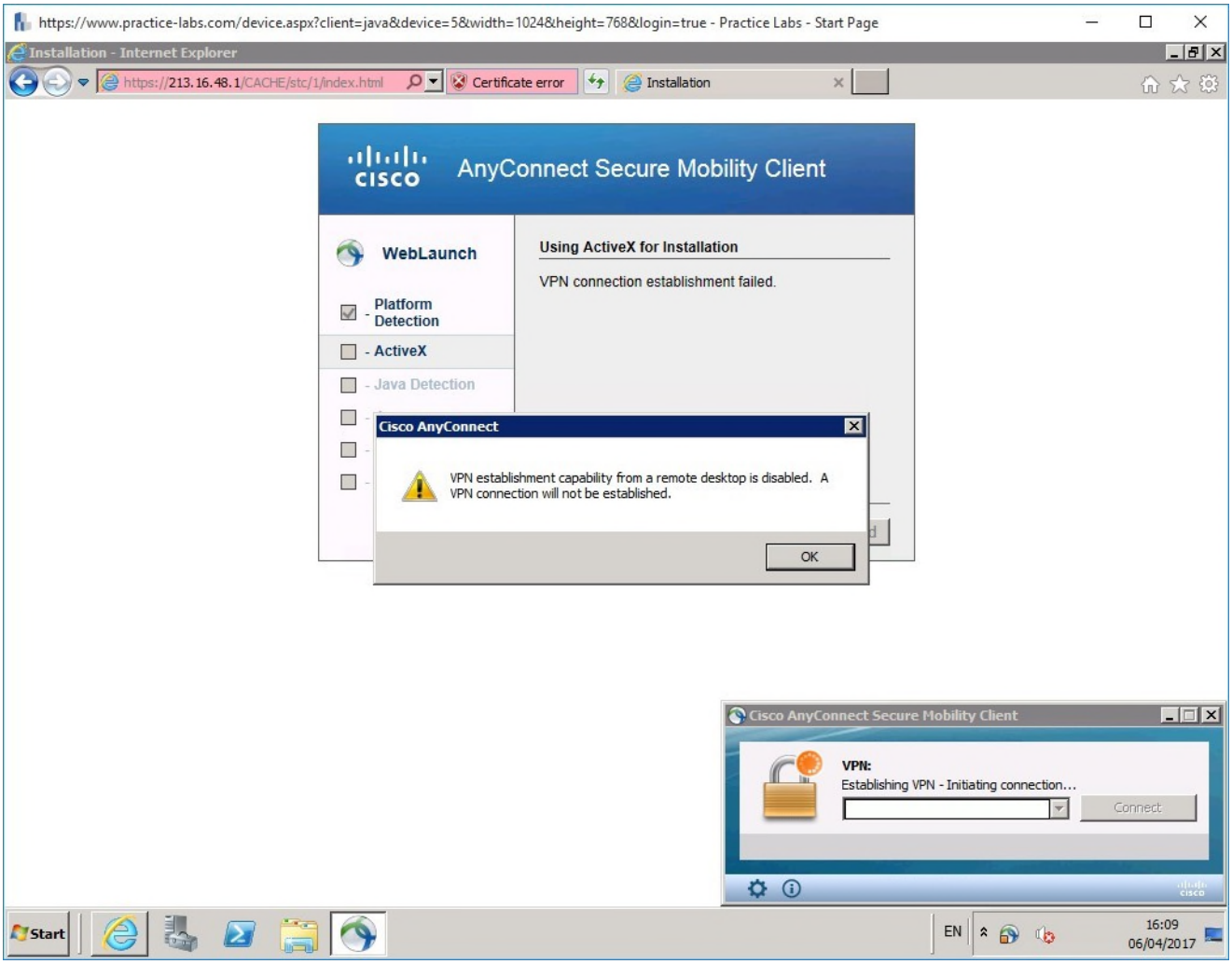


Figure 2.34 Screenshot of the Cisco AnyConnect Secure Mobility Client connection window: Notice the attempt to establish VPN connection.

Step 15

In the lab, because we are using a remote desktop connection to connect to the ASA, we need to allow this in a policy.

Flip back to **PLABMGMT** then in the ASDM navigate to **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**:

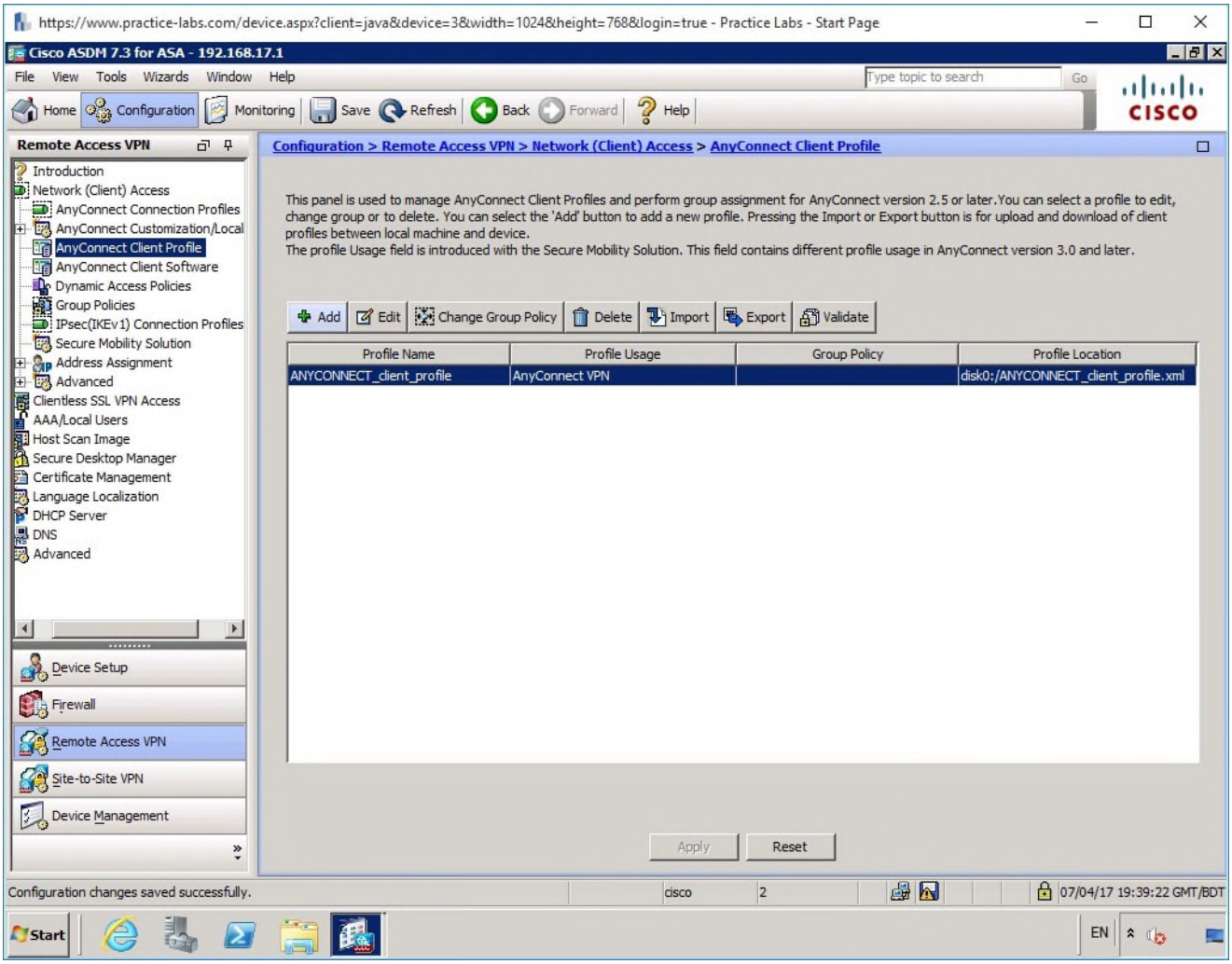


Figure 2.35 Screenshot of the AnyConnect Client Profile page: Notice the ANYCONNECT_client_profile is added.

Select the profile that is in the list, then click **Edit**.

Scroll down the options until you find Windows VPN Establishment, change this to **AllowRemoteUsers** from **Local users only**.

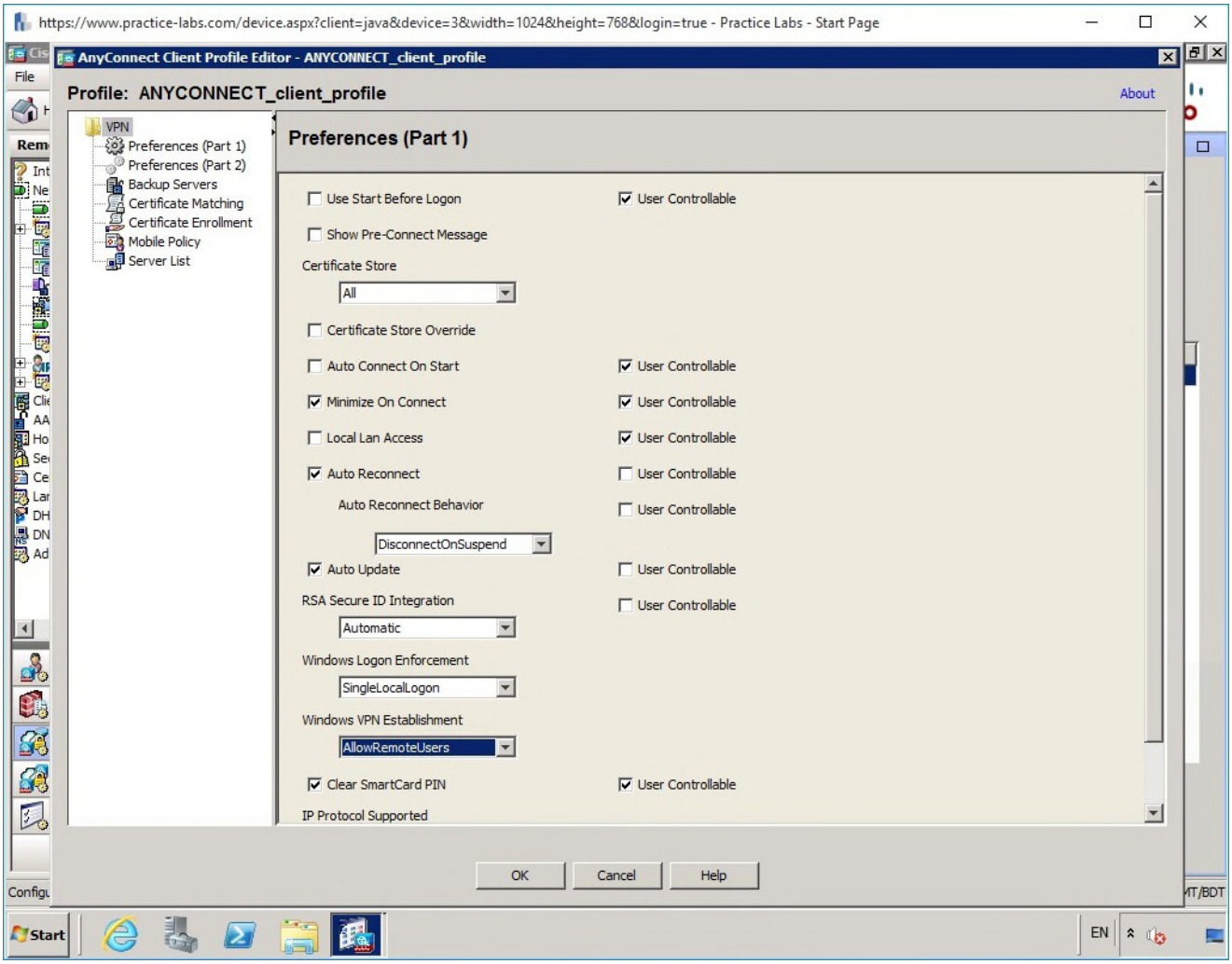


Figure 2.36 Screenshot of the Preferences (Part 1) page of the AnyConnect Client Profile Editor window: User needs ensure that in the “Windows VPN Establishment” field, the Local users only value is changed to AllowRemoteUsers.

Click **OK**, then click **Apply**.

Step 16

Flip back to **PLABEXTCLI**, then click OK to any errors or warnings that are on the page. You can also close Internet Explorer.

In the bottom right should be the Cisco AnyConnect client, if it’s not there is a new folder under **Start > All Programs > Cisco**. The client will be located here:

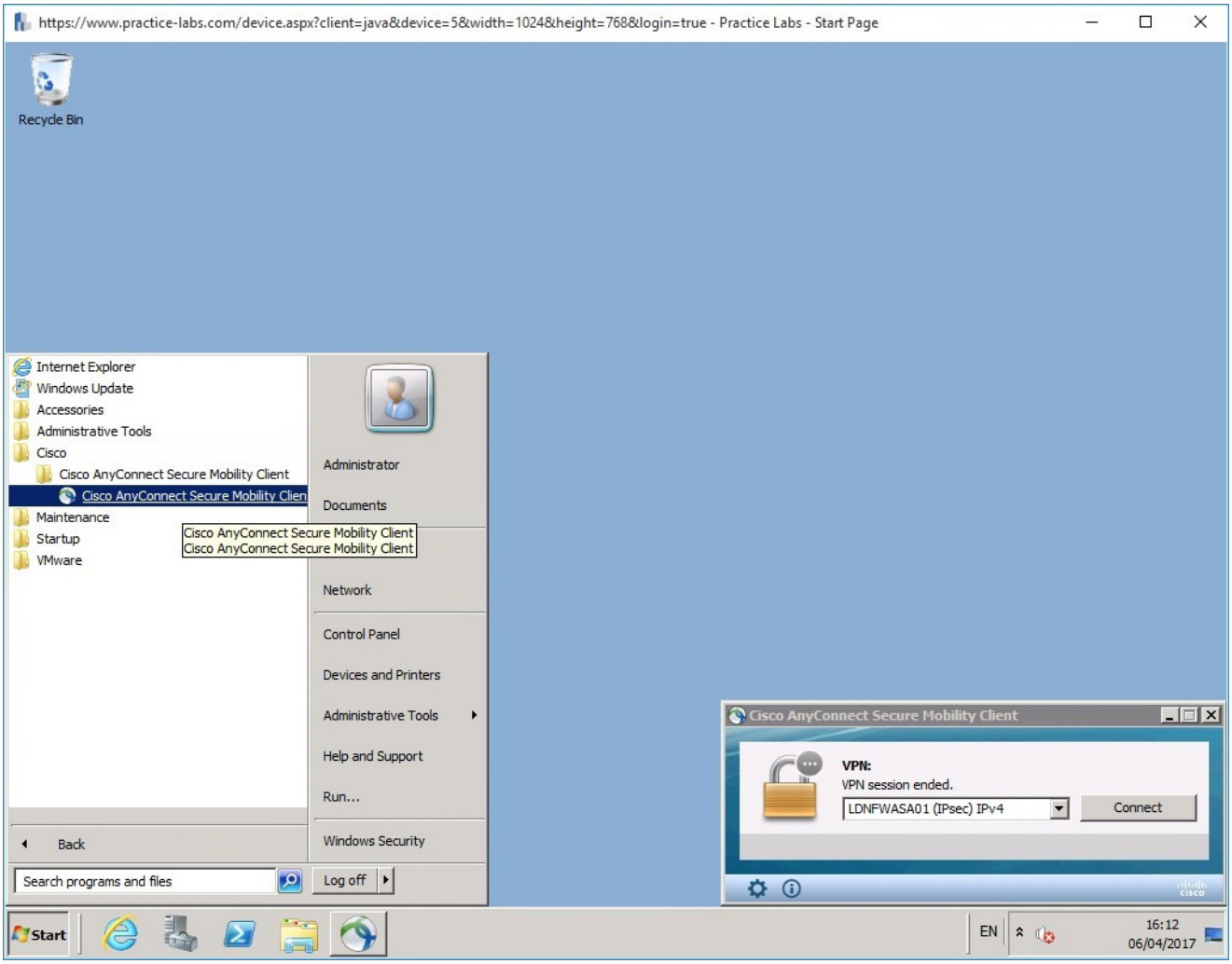


Figure 2.37 Screenshot of the Programs menu of the PLABEXTCLI window: User needs to select Cisco AnyConnect Secure Mobility Client option from the Cisco menu.

Open the client, or in the bottom left click the **Connect** button.

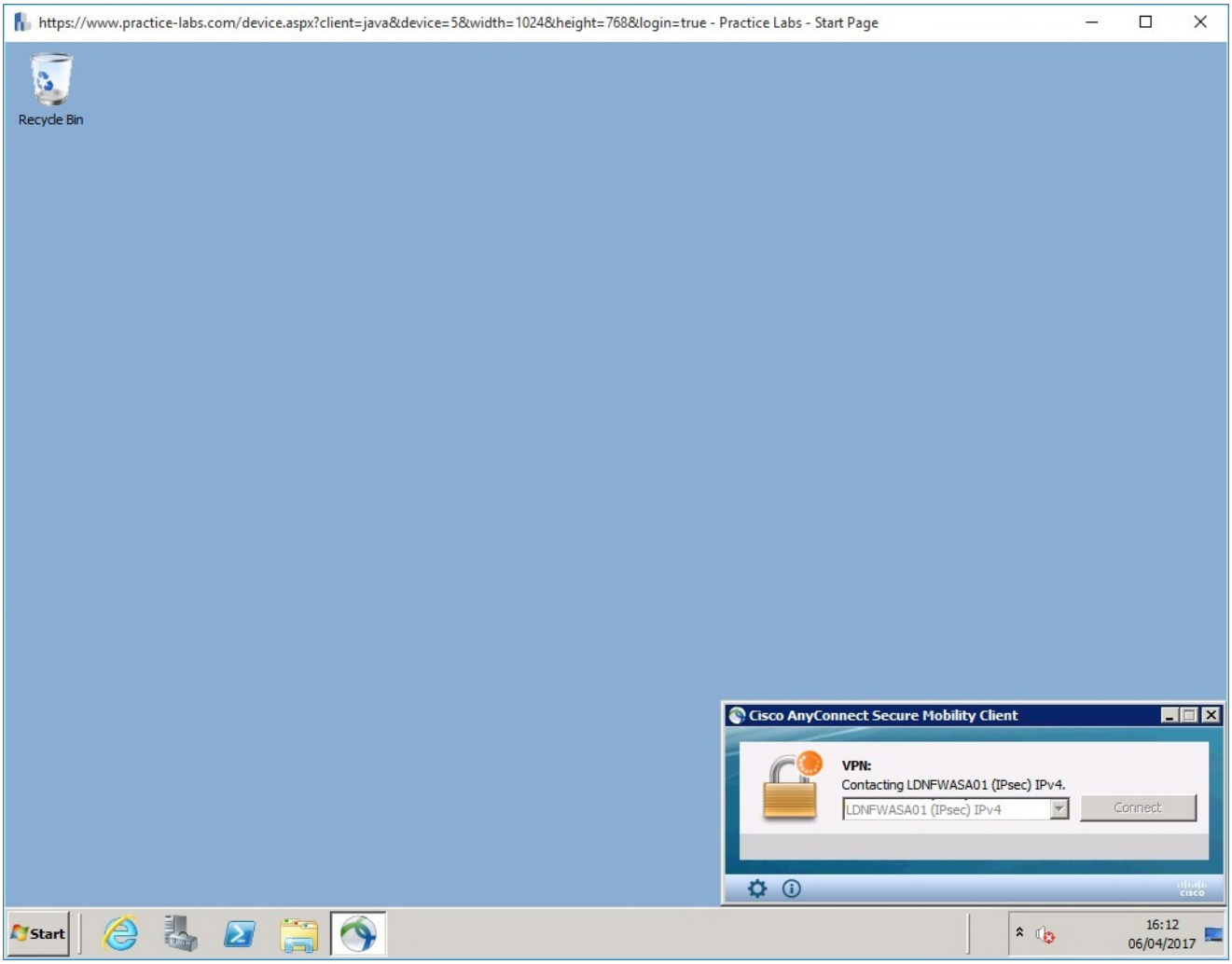


Figure 2.38 Screenshot of the Cisco AnyConnect Secure Mobility Client window: Notice the VPN server named mentioned the VPN field.

You will again see the security warning, click **Connect Anyway**:

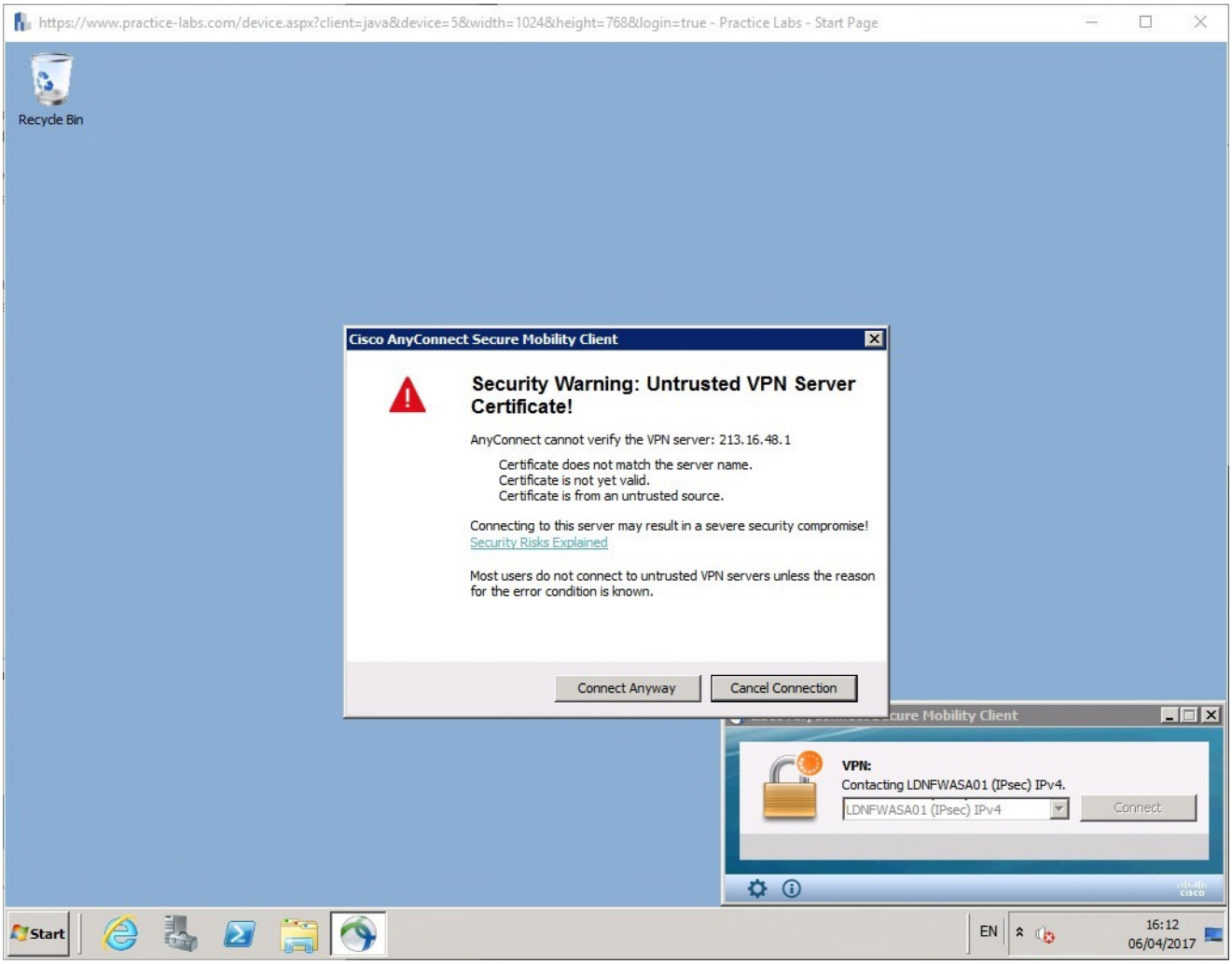


Figure 2.39 Screenshot of the Cisco AnyConnect Secure Mobility Client security warning window: User is prompted with the warning. User needs to read the warning and connect to the untrusted VPN Server.

Enter your credentials (**fred / cisco123**):

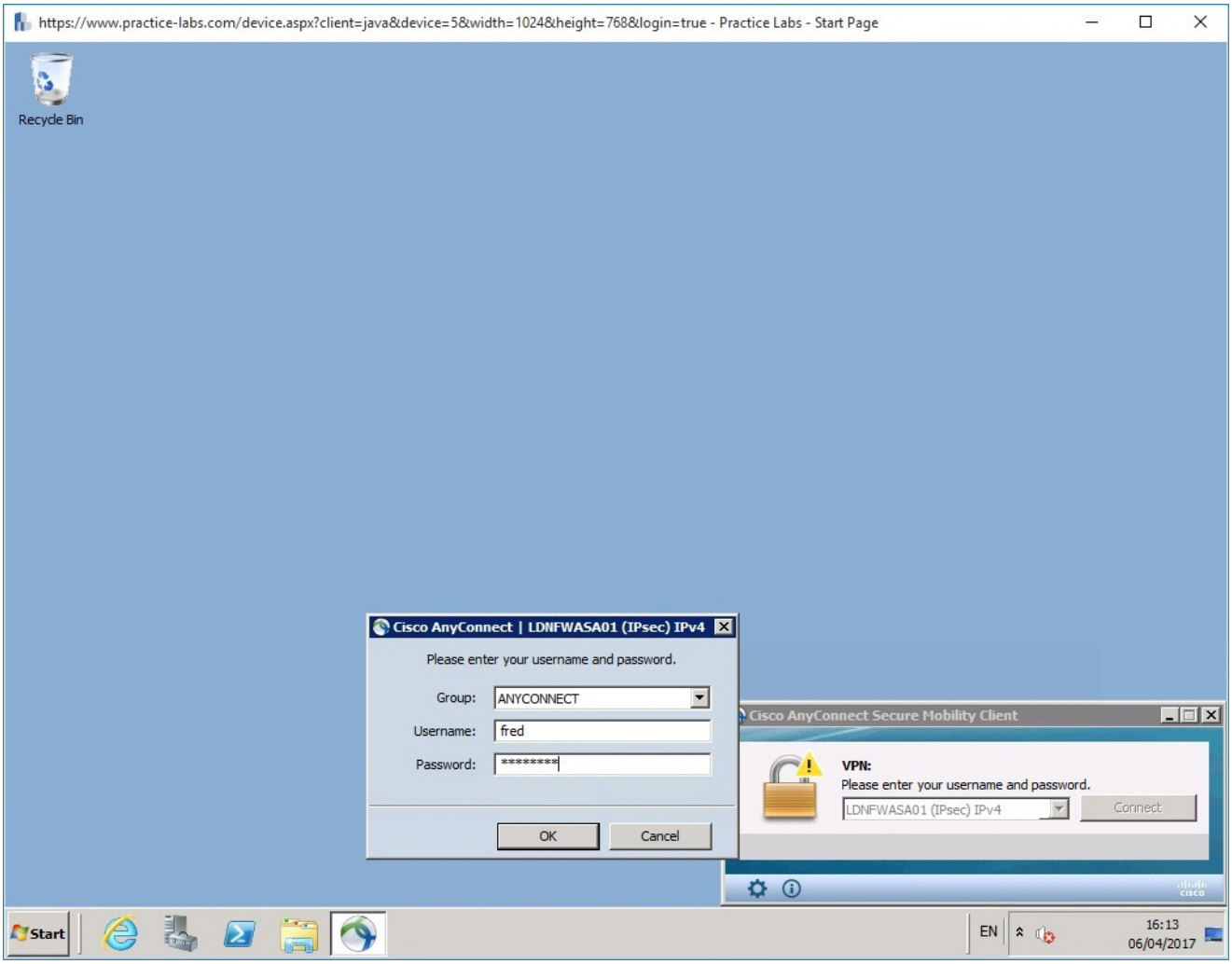


Figure 2.40 Screenshot of the Cisco AnyConnect window: User needs to enter the user credentials to connect with the VPN Server.

Press **OK**.

You may get the warning again, click **Connect Anyway**.

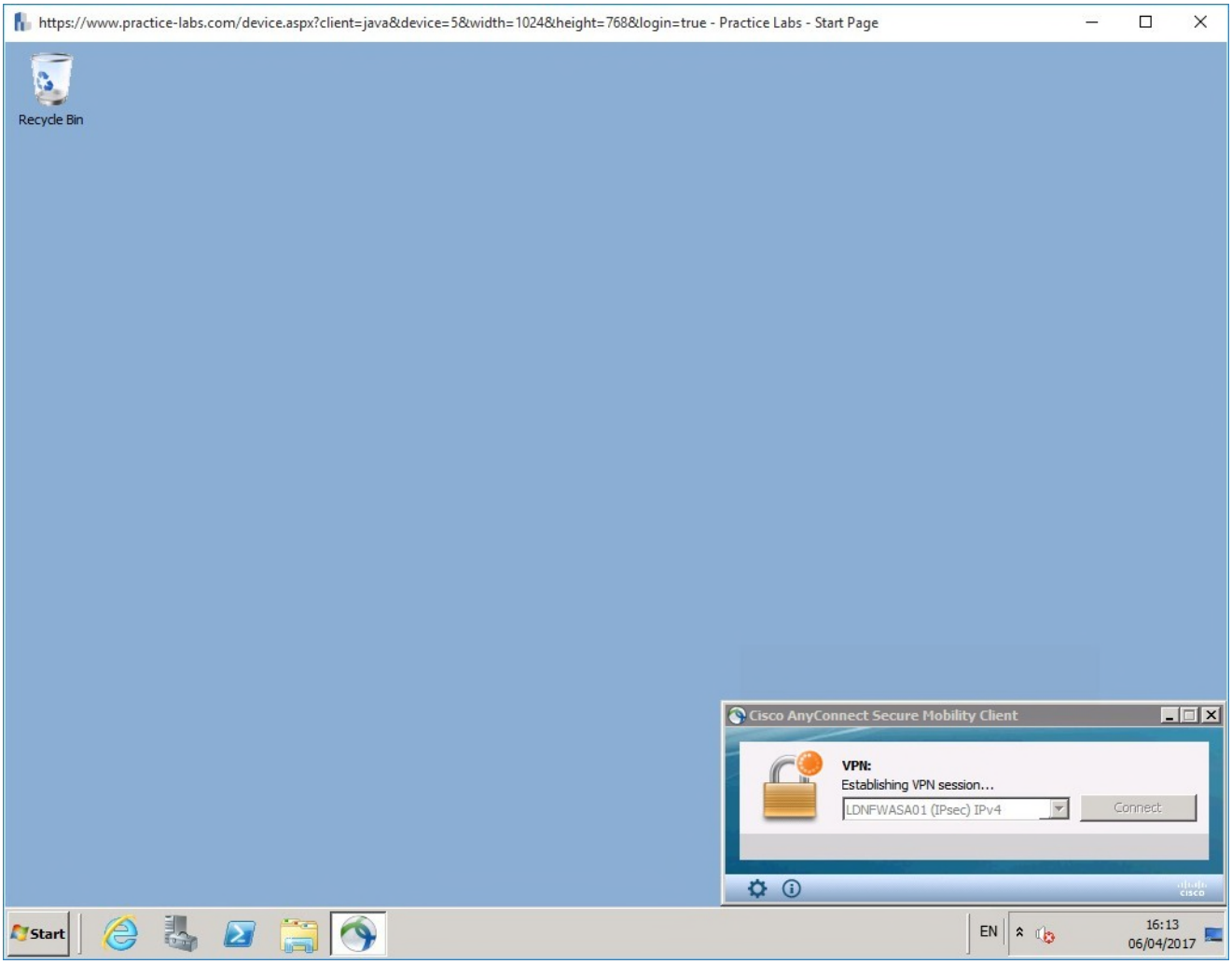


Figure 2.41 Screenshot of the Cisco AnyConnect Secure Mobility Client window: Notice that the VPN connect is being established.

You will notice that the connection freezes! This is because the routing is modified by the VPN client and you can no longer connect. After a few minutes, the RDP connection will drop (try clicking in the window or moving the mouse around).

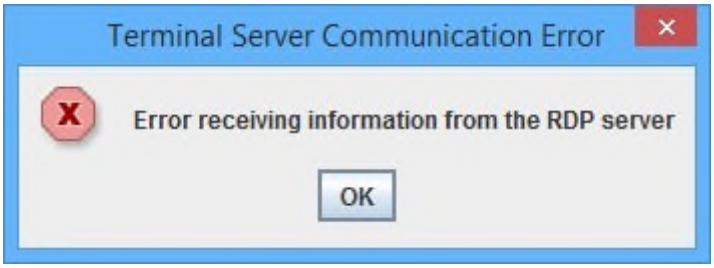


Figure 2.40 Screenshot of the Terminal Server Communication Error window: Notice that an error is generated.

Press **OK** to this error message and reconnect to PLABEXTCLI by clicking the connect button (it looks like a plug/socket combination)

If you reconnect, you will see a message from the client:

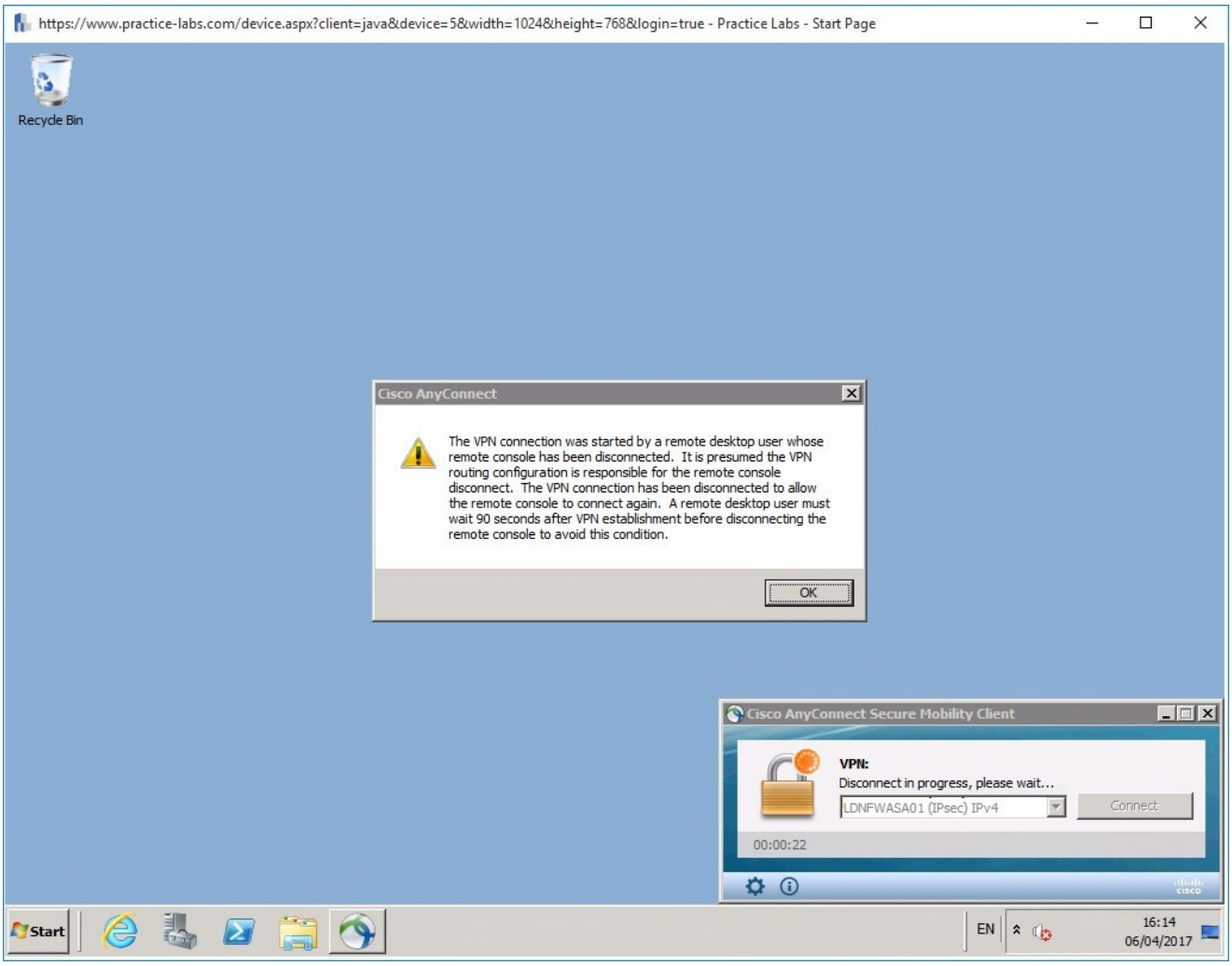


Figure 2.42 Screenshot of the Cisco AnyConnect window: Notice the error message.

To fix this issue, we need to enable split tunnelling on the client.

Step 17

To configure split tunnelling, go to PLABMGMT and in the ASDM navigate to Group Policies under Network (Client) Access.

Select the **GroupPolicy_ANYCONNECT** profile and click the **Edit** button.

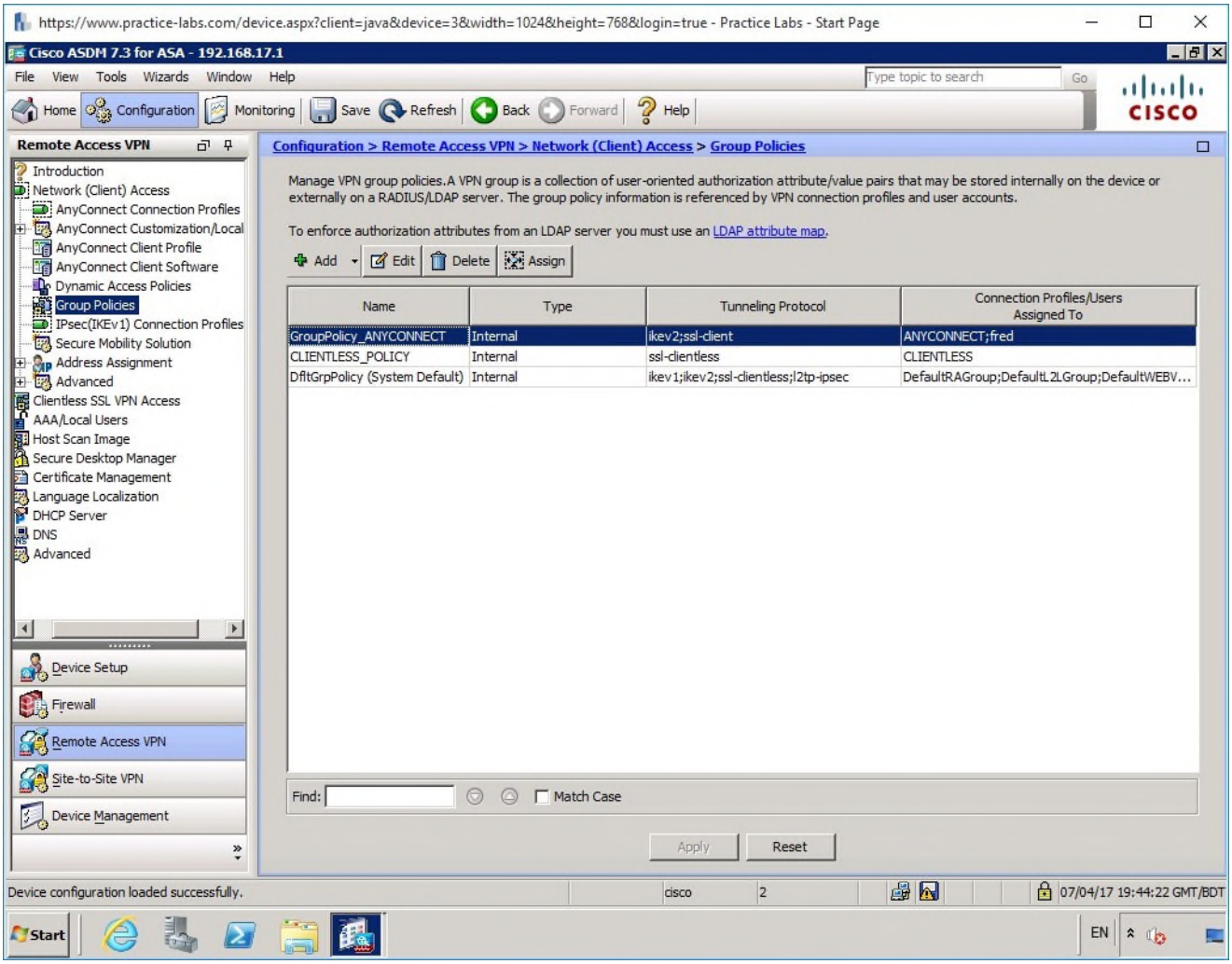


Figure 2.43 Screenshot of the Group Policies window: User needs to select GroupPolicy_ANYCONNECT to proceed further.

Step 18

Expand **Advanced** and select **Split Tunnelling**:

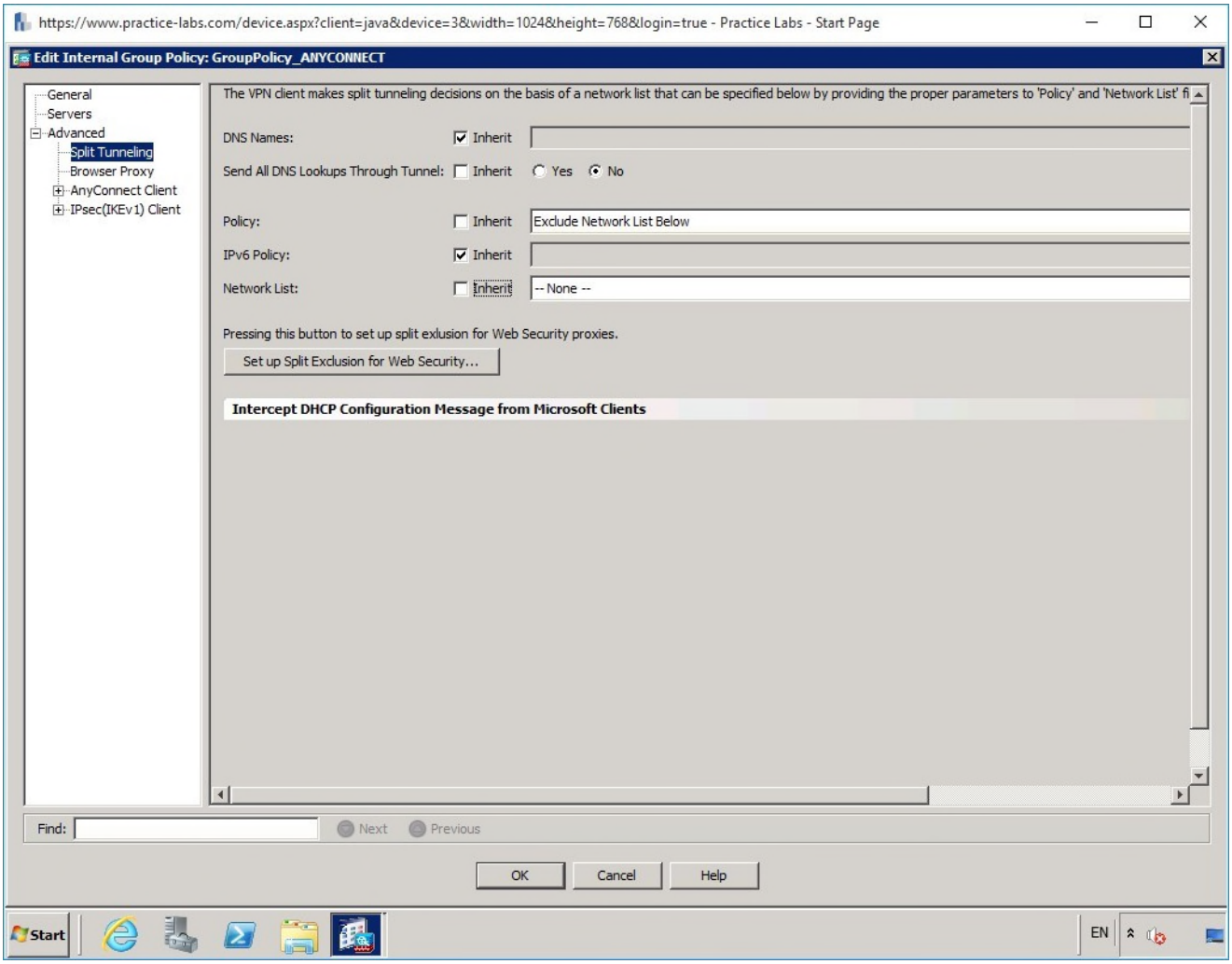


Figure 2.44 Screenshot of the Edit Internal Group Policy: GroupPolicy_ANYCONNECT window: User needs to select Split Tunneling in the left pane. The right pane will display the relevant options.

Uncheck **Policy: inherit** and Ensure Policy says **Exclude Network List Below**.

Uncheck **Network List: inherit** then scroll to the right and click the **Manage** button next to the **Network List** box.

Click the **Add** down arrow and select **Add ACL**, call it **split_tunnel**, click **OK**.

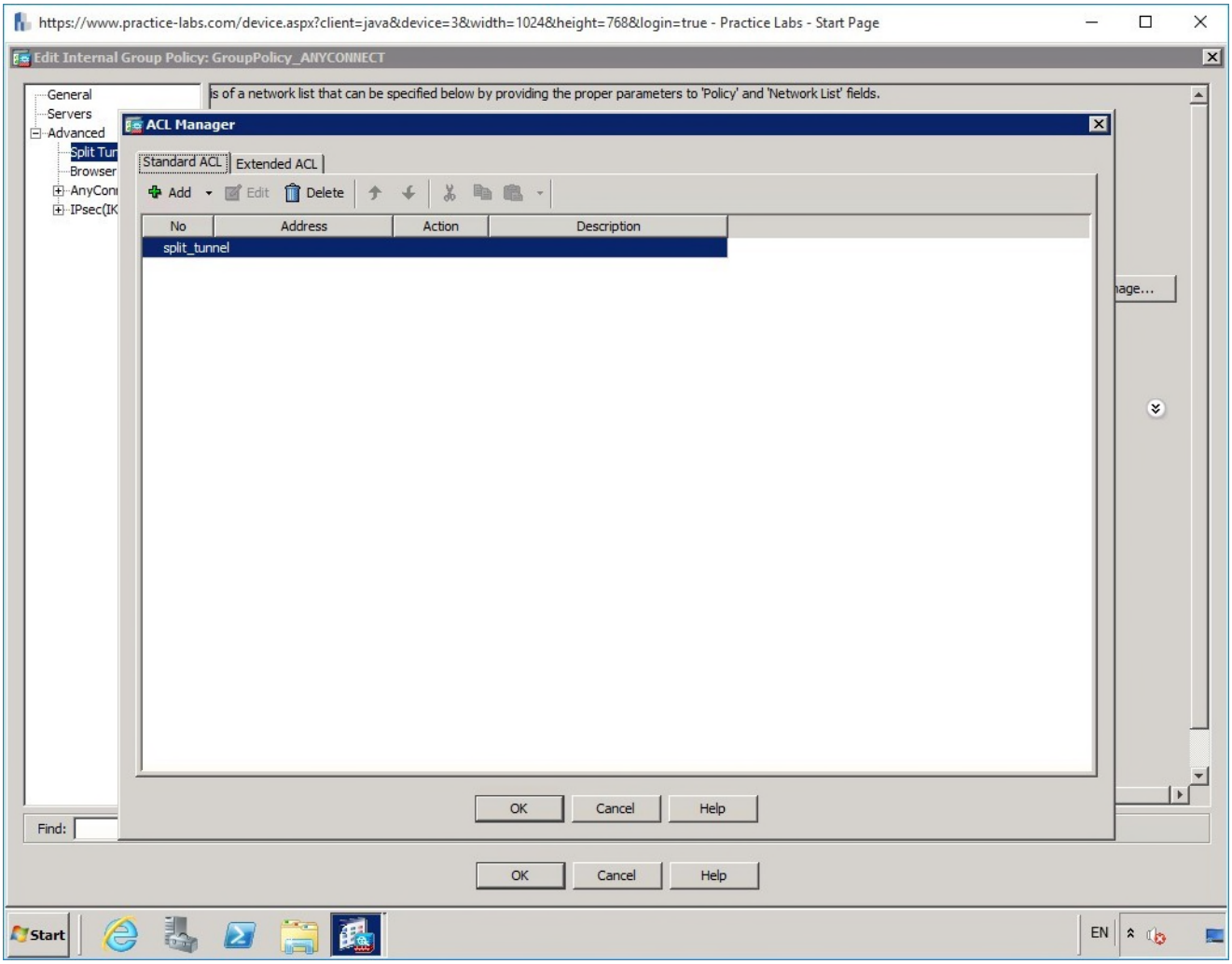


Figure 2.45 Screenshot of the ACL Manager window: User needs to select split_tunnel.

Select the ACL and the click the **Add** button down arrow again; this time, select **ACE entry**.

Enter in **10.44.24.0/24** as the address, ensure **permit** is selected and click **OK**.

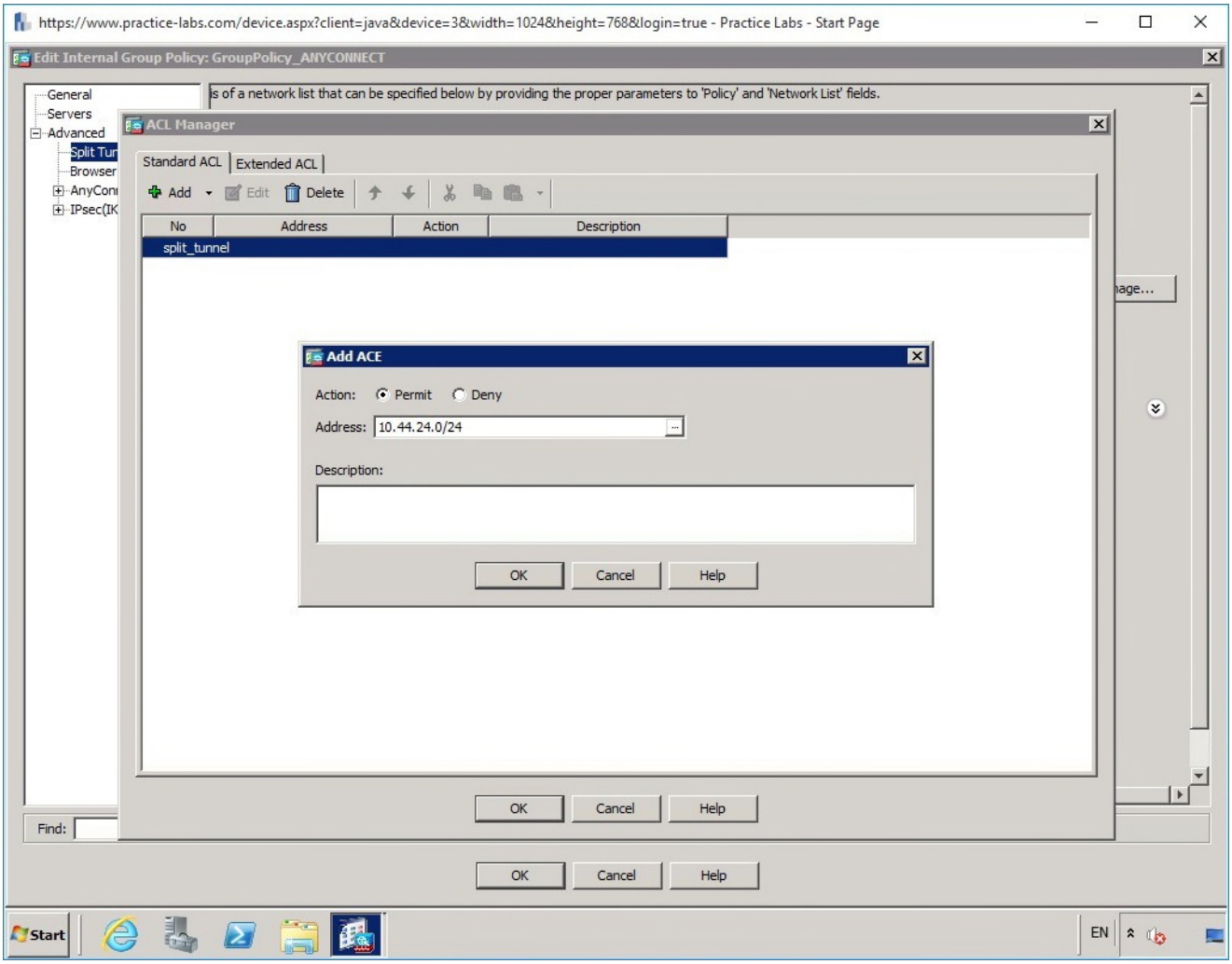


Figure 2.46 Screenshot of the Add ACE window: User needs to provide an IP address in the Address field.

Click **OK,** then **OK** to any open dialogs.

Click **Apply** when back at the main ASDM page.

Step 19

Switch back to PLABEXTCLI and reconnect the VPN again, again you will be prompted with the security warning and your credentials. As always click **Connect anyway** and enter in **fred / cisco123** as the credentials. You will notice this time that the connection succeeds:

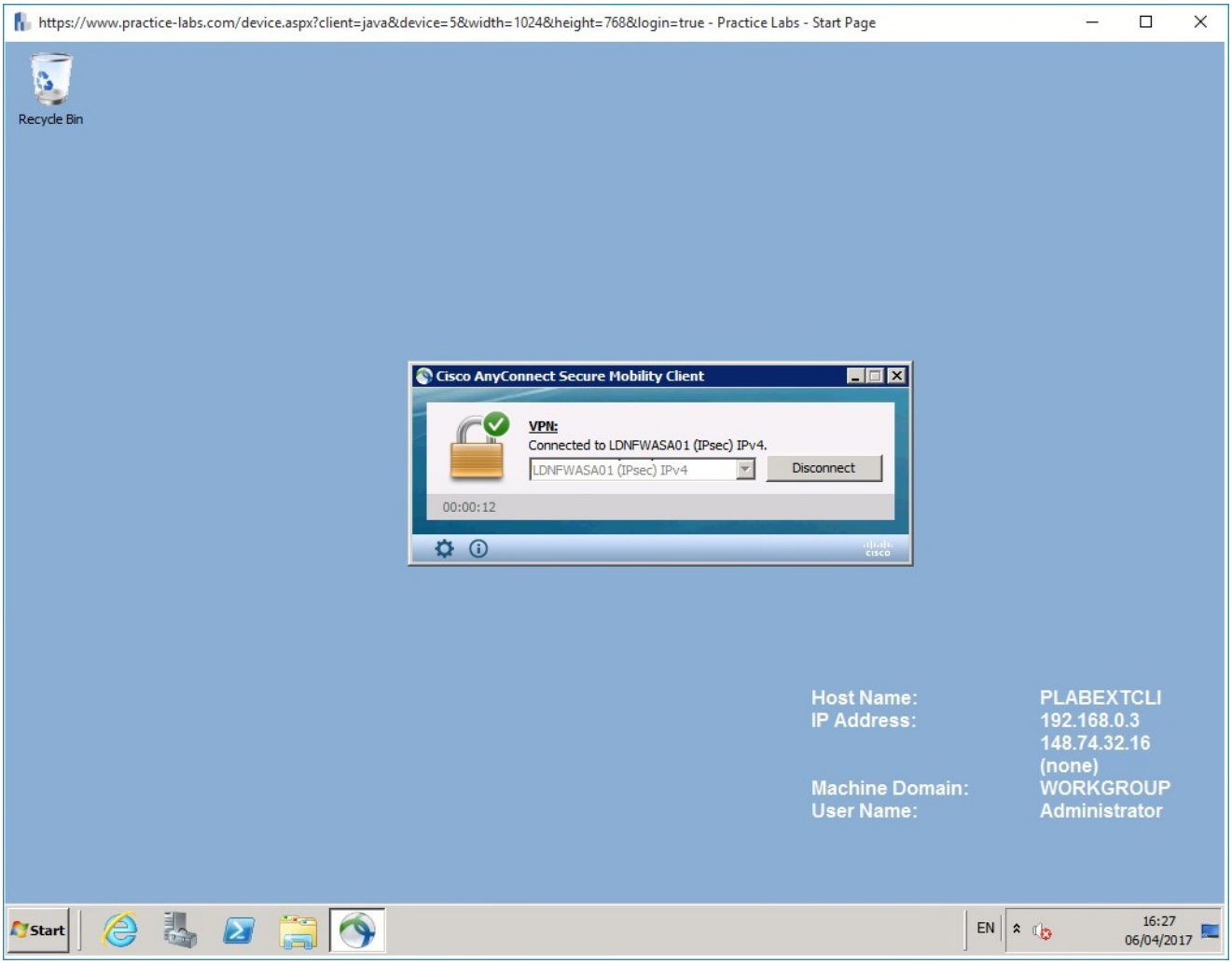


Figure 2.47 Screenshot of the Cisco AnyConnect Secure Mobility Client window: Notice that VPN is now connected.

In the real world if you have valid security certificate this installation is a little smoother. However, I think its good practice to have seen a few gotchas in this tutorial to get the client up and running!

To fully test you are connected, why not terminal services from PLABEXTCLI to PLABMGMT at 192.168.16.10:

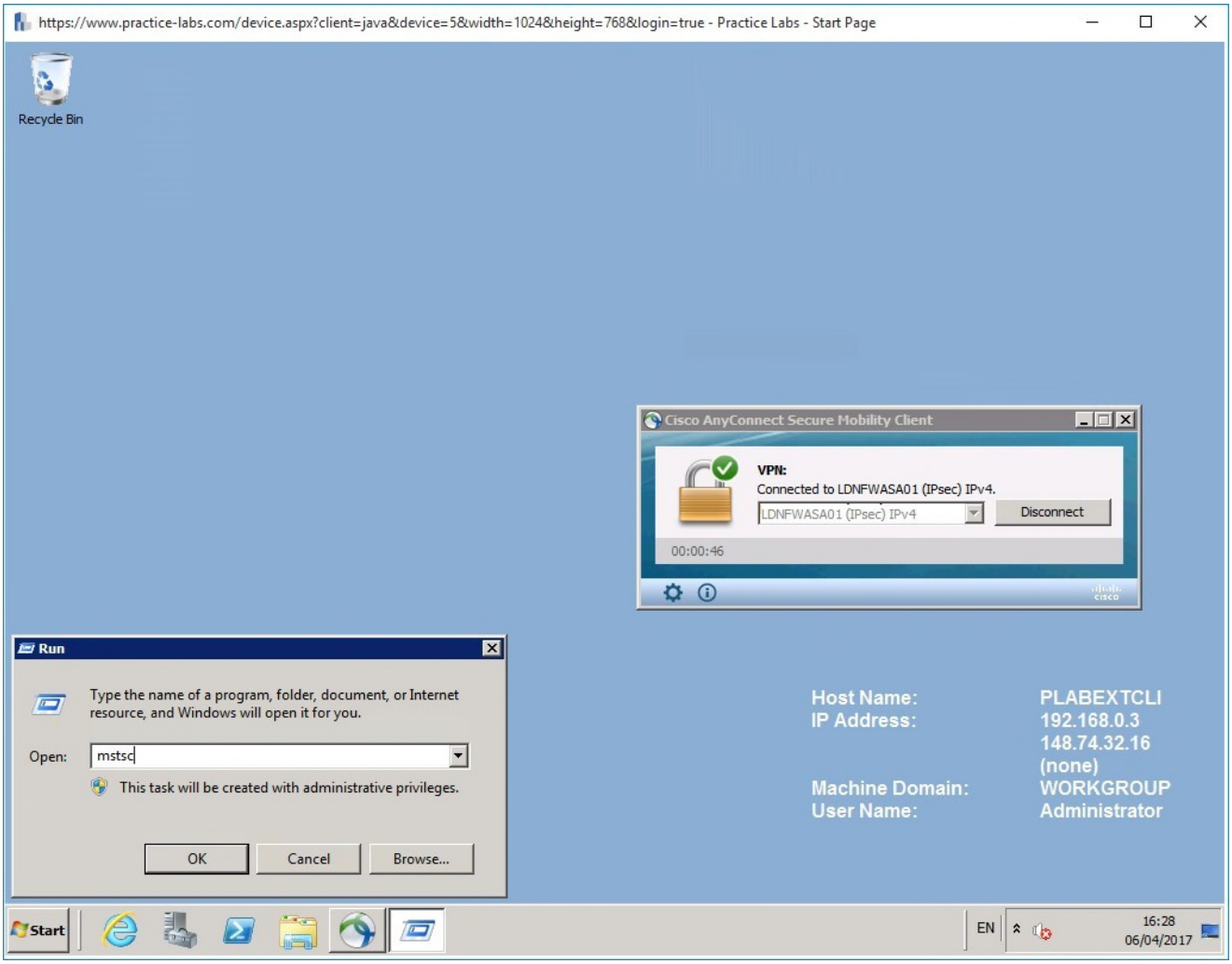


Figure 2.48 Screenshot of the Run window: User needs to enter mstsc command to invoke a remote desktop session.

Connect to 192.168.16.10:

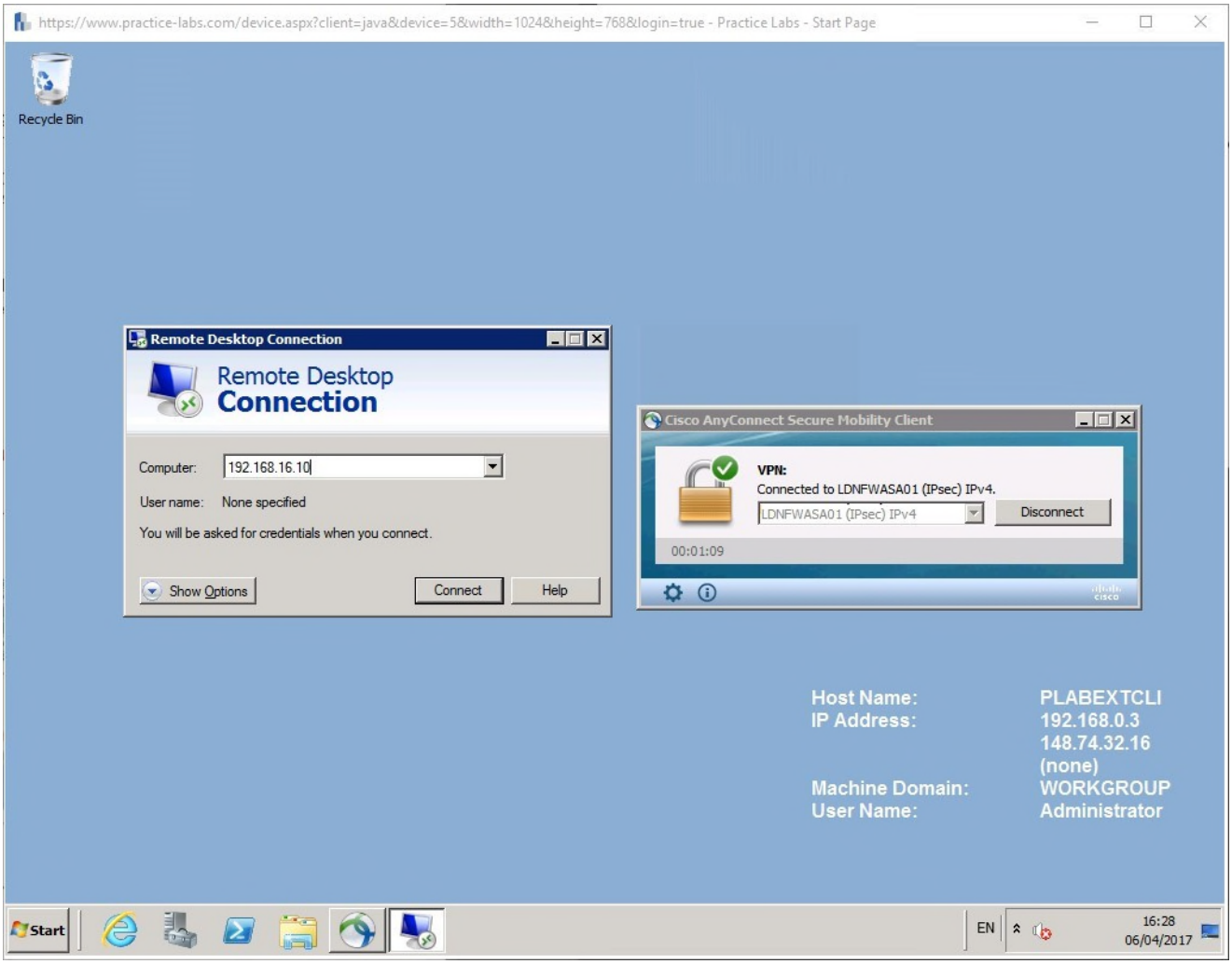


Figure 2.49 Screenshot of the Remote Desktop Connection window: User needs to enter IP address of the server to connect to in the Computer field.

Enter the credentials **Administrator** / **`Passw0rd`**

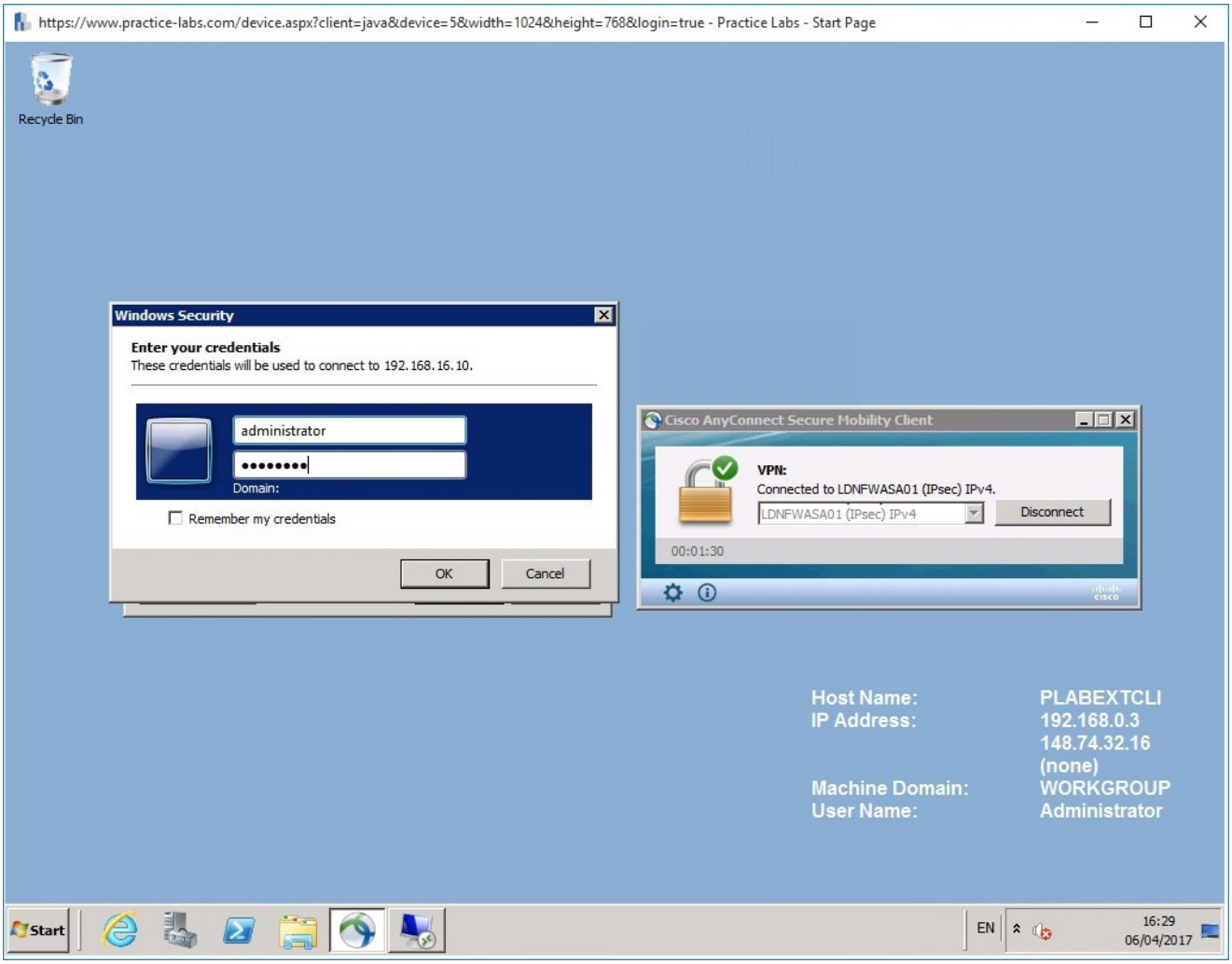


Figure 2.50 Screenshot of the Windows Security window: User needs to provide user credentials.

A certificate warning is displayed, click **Yes**:

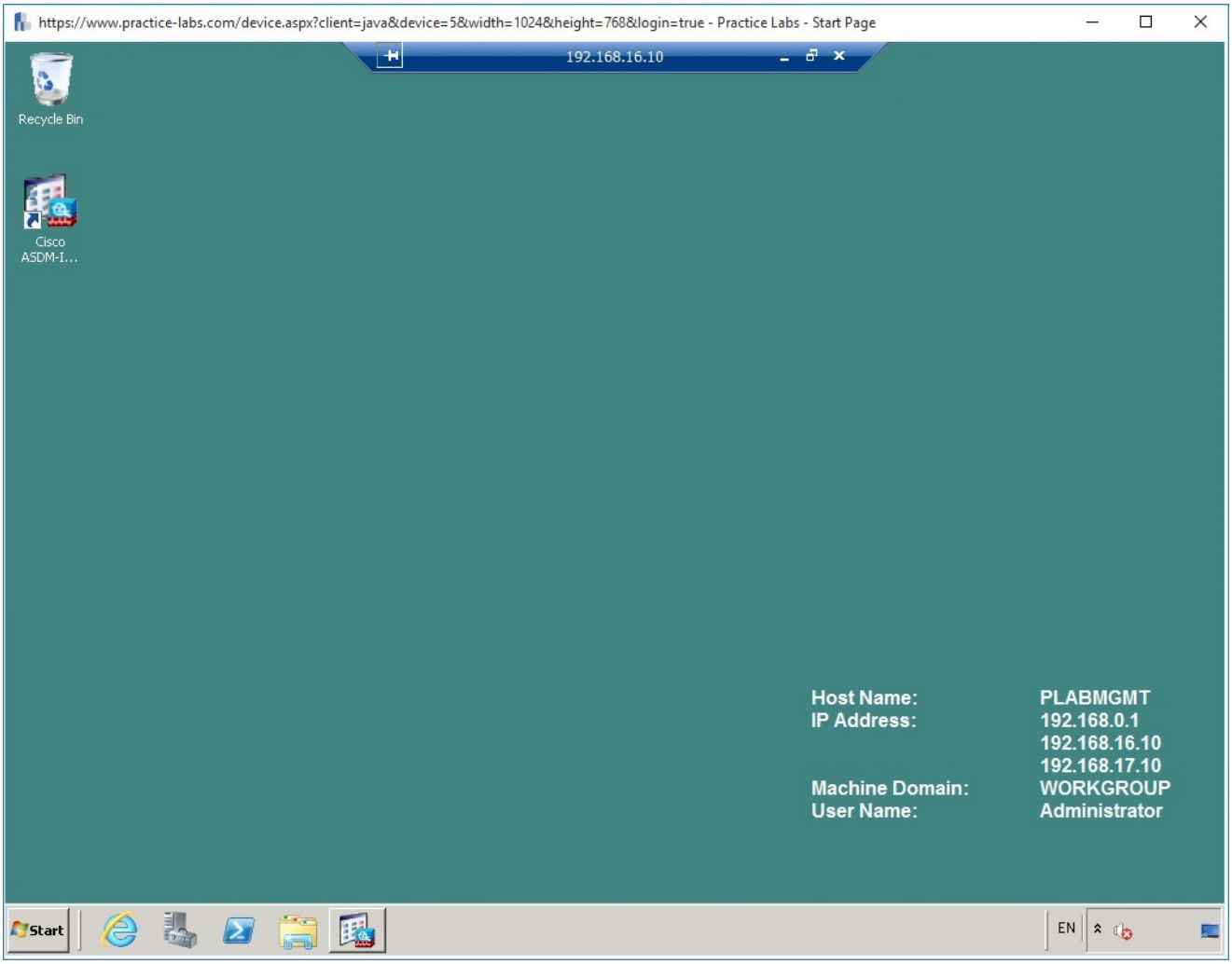


Figure 2.51 Screenshot of the 192.168.16.10 window: User is connected to the remote server.

You are now connected, proving your VPN is operational!

Summary

In this module, you configured both the Clientless SSL VPN and Cisco AnyConnect client.

The AnyConnect client has more functionality but is harder to deploy.

You covered the following activities in this module:

- Implement a Clientless SSL VPN using the Cisco ASA Device Manager
- Implement an AnyConnect using the Cisco ASA Device Manager