

Configure an External AAA Server for VPN

- About External AAA Servers, on page 1
- Guidelines For Using External AAA Servers, on page 2
- Configure Multiple Certificate Authentication, on page 2
- Active Directory/LDAP VPN Remote Access Authorization Examples, on page 3

About External AAA Servers

This ASA can be configured to use an external LDAP, RADIUS, or TACACS+ server to support Authentication, Authorization, and Accounting (AAA) for the ASA. The external AAA server enforces configured permissions and attributes. Before you configure the ASA to use an external server, you must configure the external AAA server with the correct ASA authorization attributes and, from a subset of these attributes, assign specific permissions to individual users.

Understanding Policy Enforcement of Authorization Attributes

The ASA supports several methods of applying user authorization attributes (also called user entitlements or permissions) to VPN connections. You can configure the ASA to obtain user attributes from any combination of:

- a Dynamic Access Policy (DAP) on the ASA
- an external RADIUS or LDAP authentication and/or authorization server
- a group policy on the ASA

If the ASA receives attributes from all sources, the attributes are evaluated, merged, and applied to the user policy. If there are conflicts between attributes, the DAP attributes take precedence.

The ASA applies attributes in the following order:

1. DAP attributes on the ASA—Introduced in Version 8.0(2), these attributes take precedence over all others. If you set a bookmark or URL list in DAP, it overrides a bookmark or URL list set in the group policy.
2. User attributes on the AAA server—The server returns these attributes after successful user authentication and/or authorization. Do not confuse these with attributes that are set for individual users in the local AAA database on the ASA (User Accounts in ASDM).

3. Group policy configured on the ASA—If a RADIUS server returns the value of the RADIUS CLASS attribute IETF-Class-25 (OU=*group-policy*) for the user, the ASA places the user in the group policy of the same name and enforces any attributes in the group policy that are not returned by the server.

   For LDAP servers, any attribute name can be used to set the group policy for the session. The LDAP attribute map that you configure on the ASA maps the LDAP attribute to the Cisco attribute IETF-Radius-Class.

4. Group policy assigned by the Connection Profile (called tunnel-group in the CLI)—The Connection Profile has the preliminary settings for the connection, and includes a default group policy applied to the user before authentication. All users connecting to the ASA initially belong to this group, which provides any attributes that are missing from the DAP, user attributes returned by the server, or the group policy assigned to the user.

5. Default group policy assigned by the ASA (DfltGrpPolicy)—System default attributes provide any values that are missing from the DAP, user attributes, group policy, or connection profile.

Guidelines For Using External AAA Servers

The ASA enforces the LDAP attributes based on attribute name, not numeric ID. RADIUS attributes, are enforced by numeric ID, not by name.

For ASDM Version 7.0, LDAP attributes include the cVPN3000 prefix. For ASDM Versions 7.1 and later, this prefix was removed.

LDAP attributes are a subset of the Radius attributes, which are listed in the Radius chapter.

Configure Multiple Certificate Authentication

You can now validate multiple certificates per session with the AnyConnect Client SSL and IKEv2 client protocols. For example, you can make sure that the issuer name of the machine certificate matches a particular CA and therefore that the device is a corporate-issued device.

The multiple certificates option allows certificate authentication of both the machine and user via certificates. Without this option, you could only do certificate authentication of one or the other, but not both.



Note Because multiple certificate authentication requires a machine certificate and a user certificate (or two user certificates), you cannot use AnyConnect Client start before logon (SBL) with this feature.

The pre-fill username field allows a field from the second (user) certificate to be parsed and used for subsequent AAA authentication in a AAA and certificate authenticated connection. The username for both primary and secondary prefill is always retrieved from the second (user) certificate received from the client.

Beginning with 9.14(1), ASA allows you to specify which certificate the primary and secondary username should come from when configuring multiple certificate authentication and using the pre-fill username option for Authentication or Authorization. For information, see AnyConnect Client Connection Profile, Authentication Attributes

With multiple certificate authentication, two certificates are authenticated: the second (user) certificate received from the client is the one that the pre-fill and username-from-certificate primary and secondary usernames are parsed from.

You can also configure multiple certificate authentication with SAML.

With multiple-certificate authentication, you can make policy decisions based on the fields of a certificate used to authenticate that connection attempt. The user and machine certificate received from the client during multiple-certificate authentication is loaded into DAP to allow policies to be configured based on the field of the certificate. To add multiple certificate authentication using Dynamic Access Policies (DAP) so that you can set up rules to allow or disallow connection attempts, refer to *Add Multiple Certificate Authentication to DAP* in the appropriate release of the ASA VPN ASDM Configuration Guide.

Active Directory/LDAP VPN Remote Access Authorization Examples

This section presents example procedures for configuring authentication and authorization on the ASA using the Microsoft Active Directory server. It includes the following topics:

- Policy Enforcement of User-Based Attributes, on page 3
- Enforce Static IP Address Assignment for AnyConnect Client Tunnels, on page 5
- Enforce Dial-in Allow or Deny Access, on page 6
- Enforce Logon Hours and Time-of-Day Rules, on page 9

Other configuration examples available on Cisco.com include the following TechNotes.

- ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example
- PIX/ASA 8.0: Use LDAP Authentication to Assign a Group Policy at Login

Policy Enforcement of User-Based Attributes

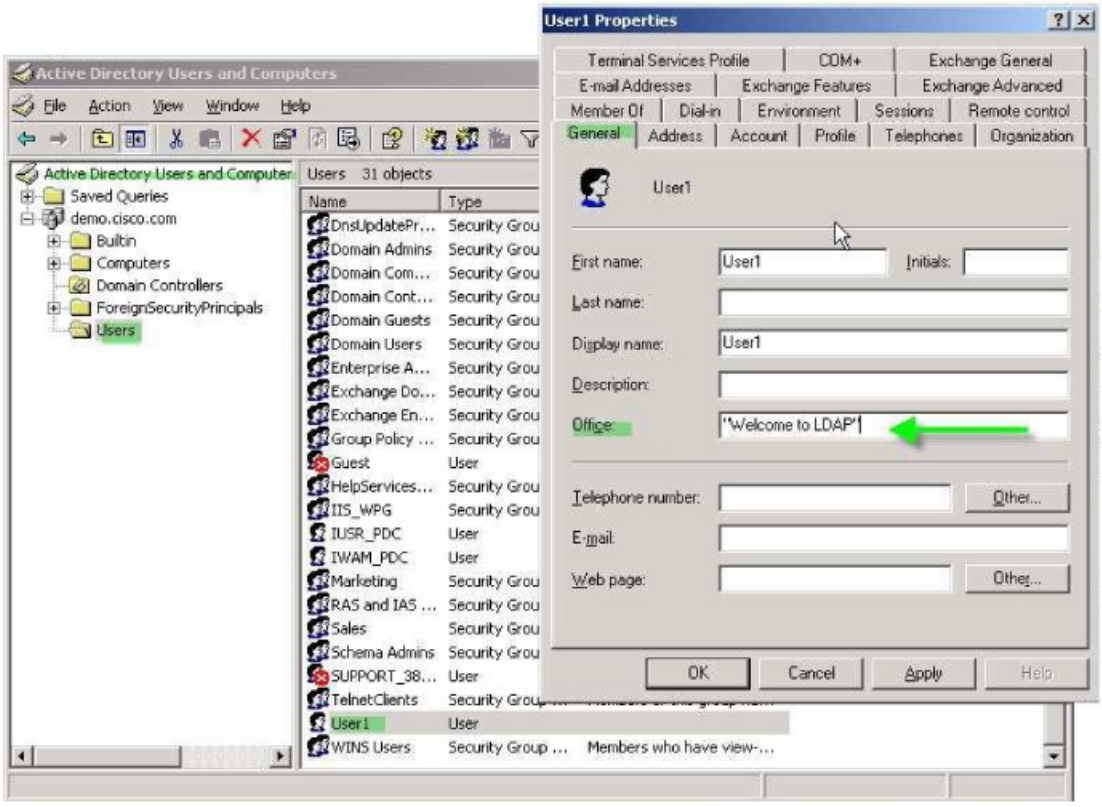
This example displays a simple banner to the user, showing how you can map any standard LDAP attribute to a well-known Vendor-Specific Attribute (VSA), and you can map one or more LDAP attribute(s) to one or more Cisco LDAP attributes. It applies to any connection type, including the IPsec VPN client and AnyConnect Client.

To enforce a simple banner for a user who is configured on an AD LDAP server use the Office field in the General tab to enter the banner text. This field uses the attribute named physicalDeliveryOfficeName. On the ASA, create an attribute map that maps physicalDeliveryOfficeName to the Cisco attribute Banner1.

During authentication, the ASA retrieves the value of physicalDeliveryOfficeName from the server, maps the value to the Cisco attribute Banner1, and displays the banner to the user.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **General** tab and enter banner text in the Office field, which uses the AD/LDAP attribute physicalDeliveryOfficeName.



Step 2 Create an LDAP attribute map on the ASA.

Create the map Banner and map the AD/LDAP attribute physicalDeliveryOfficeName to the Cisco attribute Banner1:

```
hostname(config)# ldap attribute-map Banner
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Banner1
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP, and associate the attribute map Banner that you previously created:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map Banner
```

Step 4 Test the banner enforcement.

Enforce Static IP Address Assignment for AnyConnect Client Tunnels

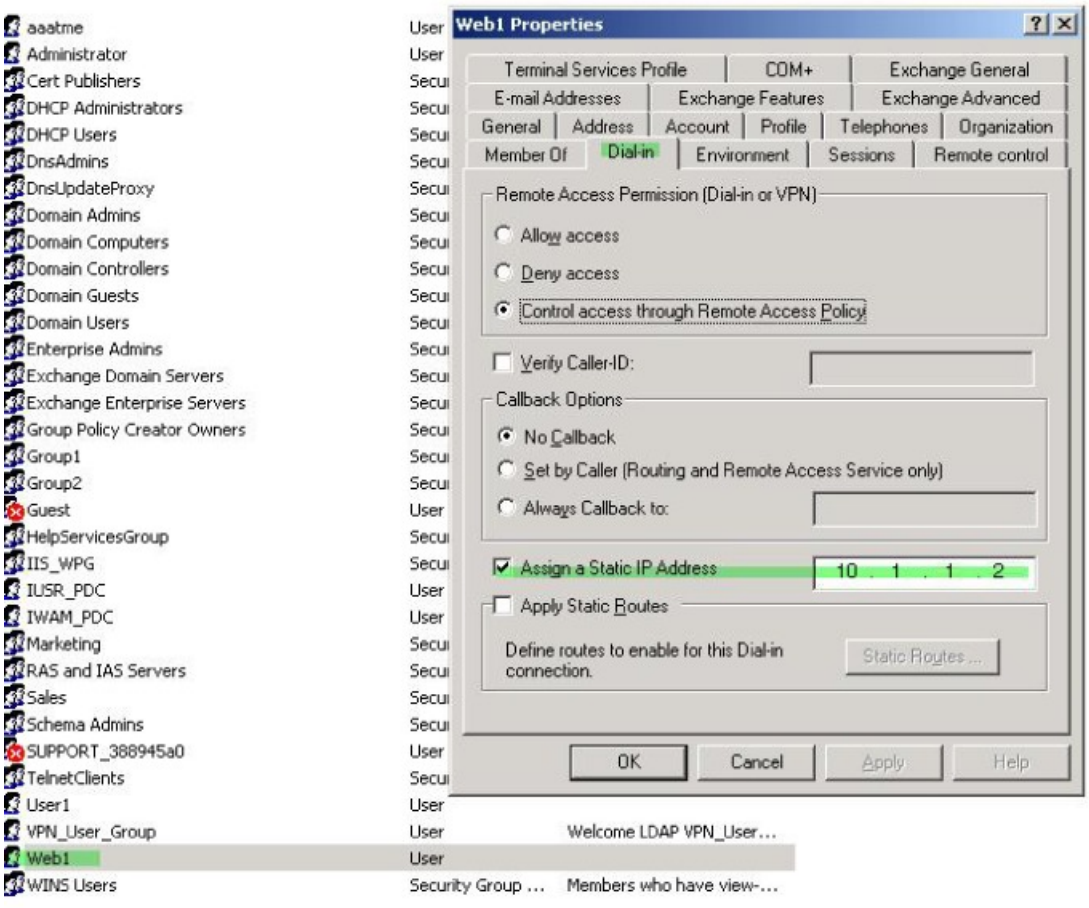
This example applies to full-tunnel clients, such as the IPsec client and the SSL VPN clients.

To enforce static AnyConnect Client static IP assignments configure the AnyConnect Client user Web1 to receive a static IP address, enter the address in the Assign Static IP Address field of the Dialin tab on the AD LDAP server (this field uses the msRADIUSFramedIPAddress attribute), and create an attribute map that maps this attribute to the Cisco attribute IETF-Radius-Framed-IP-Address.

During authentication, the ASA retrieves the value of msRADIUSFramedIPAddress from the server, maps the value to the Cisco attribute IETF-Radius-Framed-IP-Address, and provides the static address to User1.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **Dial-in** tab, check the **Assign Static IP Address** check box, and enter an IP address of 10.1.1.2.



Step 2 Create an attribute map for the LDAP configuration shown.

Map the AD attribute msRADIUSFramedIPAddress used by the Static Address field to the Cisco attribute IETF-Radius-Framed-IP-Address:

```
hostname(config)# ldap attribute-map static_address
hostname(config-ldap-attribute-map)# map-name msRADIUSFramedIPAddress
IETF-Radius-Framed-IP-Address
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP, and associates the attribute map static_address that you previously created in:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map static_address
```

Step 4 Verify that the **vpn-address-assignment** command is configured to specify AAA by viewing this part of the configuration:

```
hostname(config)# show run all vpn-addr-assign
vpn-addr-assign aaa   << Make sure this is configured >>
no vpn-addr-assign dhcp
vpn-addr-assign local
hostname(config)#
```

Step 5 Establish a connection to the ASA with the AnyConnect Client. Observe that the user receives the IP address configured on the server and mapped to the ASA.

Step 6 Use the **show vpn-sessiondb svc** command to view the session details and verify the address assigned:

```
hostname# show vpn-sessiondb svc

Session Type: SVC
Username     : web1                   Index        : 31
Assigned IP  : 10.1.1.2              Public IP    : 10.86.181.70
Protocol     : Clientless SSL-Tunnel DTLS-Tunnel
Encryption   : RC4 AES128             Hashing      : SHA1
Bytes Tx     : 304140                 Bytes Rx     : 470506
Group Policy : VPN_User_Group         Tunnel Group : Group1_TunnelGroup
Login Time   : 11:13:05 UTC Tue Aug 28 2007
Duration     : 0h:01m:48s
NAC Result   : Unknown
VLAN Mapping : N/A                    VLAN         : none
```

Enforce Dial-in Allow or Deny Access

This example creates an LDAP attribute map that specifies the tunneling protocols allowed by the user. You map the allow access and deny access settings on the Dialin tab to the Cisco attribute Tunneling-Protocol, which supports the following bitmap values:

Value	Tunneling Protocol
1	PPTP
2	L2TP
4	IPsec (IKEv1)
8	L2TP/IPsec
16	Clientless SSL
32	SSL client—AnyConnect Client or SSL VPN client
64	IPsec (IKEv2)

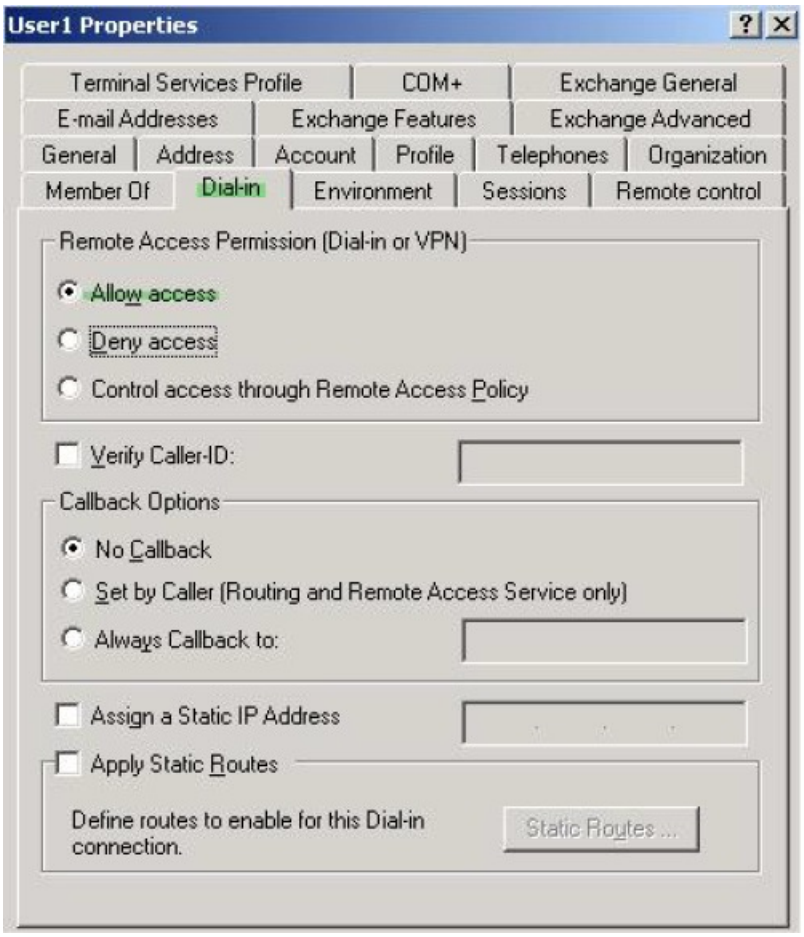
[1] (1) IPsec and L2TP over IPsec are not supported simultaneously. Therefore, the values 4 and 8 are mutually exclusive.
[2] (2) See note 1.

Use this attribute to create an Allow Access (TRUE) or a Deny Access (FALSE) condition for the protocols, and enforce the method for which the user is allowed access.

See Tech Note ASA/PIX: Mapping VPN Clients to VPN Group Policies Through LDAP Configuration Example for another example of enforcing dial-in allow access or deny access.

Procedure

Step 1 Right-click the username, open the Properties dialog box then the **Dial-in** tab, and click the Allow Access radio button.



Note
If you choose the Control access through the Remote Access Policy option, then a value is not returned from the server, and the permissions that are enforced are based on the internal group policy settings of the ASA.

Step 2 Create an attribute map to allow both an IPsec and AnyConnect Client connection, but deny a clientless SSL connection.

a) Create the map tunneling_protocols:

```
hostname(config)# ldap attribute-map tunneling_protocols
```

b) Map the AD attribute msNPAllowDialin used by the Allow Access setting to the Cisco attribute Tunneling-Protocols:

```
hostname(config-ldap-attribute-map)# map-name msNPAllowDialin Tunneling-Protocols
```

c) Add map values:

```
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin FALSE 48
hostname(config-ldap-attribute-map)# map-value msNPAllowDialin TRUE 4
```

Step 3 Associate the LDAP attribute map to the AAA server.

a) Enter the aaa server host configuration mode for the host 10.1.1.2 in the AAA server group MS_LDAP:

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
```

b) Associates the attribute map tunneling_protocols that you created:

```
hostname(config-aaa-server-host)# ldap-attribute-map tunneling_protocols
```

Step 4 Verify that the attribute map works as configured.

Try connections using clientless SSL, the user should be informed that an unauthorized connection mechanism was the reason for the failed connection. The IPsec client should connect because IPsec is an allowed tunneling protocol according to the attribute map.

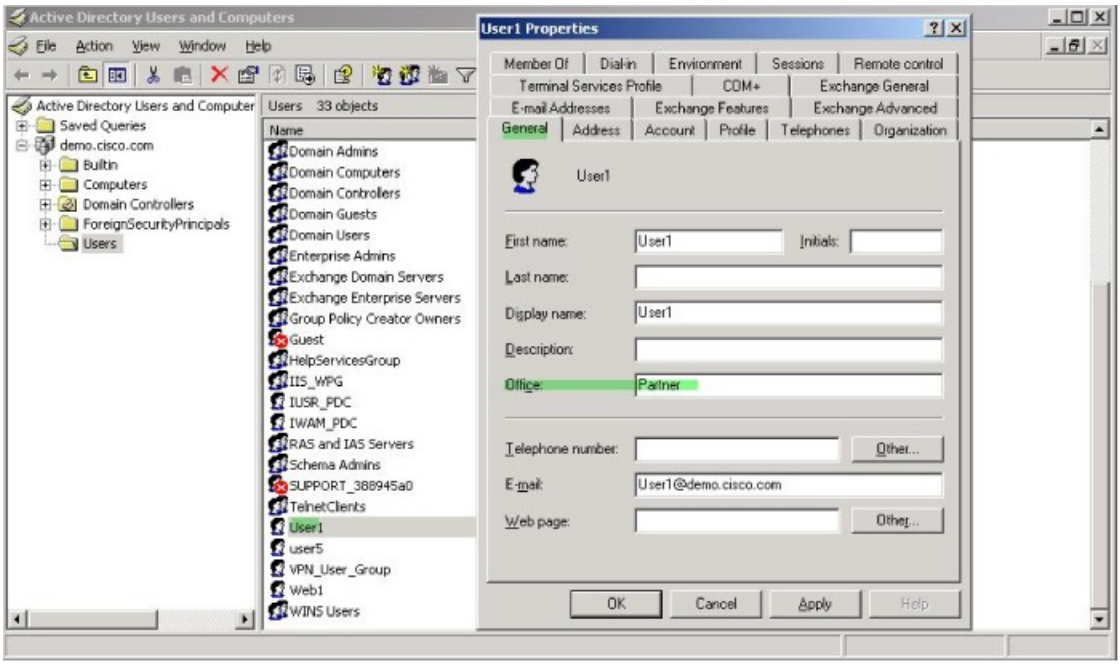
Enforce Logon Hours and Time-of-Day Rules

The following example shows how to configure and enforce the hours that a clientless SSL user (such as a business partner) is allowed to access the network.

On the AD server, use the Office field to enter the name of the partner, which uses the physicalDeliveryOfficeName attribute. Then we create an attribute map on the ASA to map that attribute to the Cisco attribute Access-Hours. During authentication, the ASA retrieves the value of physicalDeliveryOfficeName and maps it to Access-Hours.

Procedure

Step 1 Select the user, right-click **Properties**, and open the **General** tab:



Step 2 Create an attribute map.

Create the attribute map access_hours and map the AD attribute physicalDeliveryOfficeName used by the Office field to the Cisco attribute Access-Hours.

```
hostname(config)# ldap attribute-map access_hours
hostname(config-ldap-attribute-map)# map-name physicalDeliveryOfficeName Access-Hours
```

Step 3 Associate the LDAP attribute map to the AAA server.

Enter the aaa server host configuration mode for host 10.1.1.2 in the AAA server group MS_LDAP and associate the attribute map access_hours that you created.

```
hostname(config)# aaa-server MS_LDAP host 10.1.1.2
hostname(config-aaa-server-host)# ldap-attribute-map access_hours
```

Step 4 Configure time ranges for each value allowed on the server.

Configure Partner access hours from 9am to 5pm Monday through Friday:

```
hostname(config)# time-range Partner
hostname(config-time-range)# periodic weekdays 09:00 to 17:00
```