Internet Authentication Service (IAS) Installation

How to install IAS in Active Directory:
1. Add IAS service from windows component.
2. Open IAS from administrative tools.

3. Add new radius client. Follow these steps:

   **New RADIUS Client**

   **Name and Address**

   Type a friendly name and either an IP Address or DNS name for the client.

<table>
<thead>
<tr>
<th>Friendly name:</th>
<th>Aruba</th>
</tr>
</thead>
<tbody>
<tr>
<td>Client address (IP or DNS):</td>
<td>10.230.235.2</td>
</tr>
</tbody>
</table>
New RADIUS Client

Additional Information

If you are using remote access policies based on the client vendor attribute, specify the vendor of the RADIUS client:

Client-Vendor:  
RADIUS Standard

Shared secret:  

Confirm shared secret:  

Request must contain the Message Authenticator attribute

Internet Authentication Service

<table>
<thead>
<tr>
<th>Service Name</th>
<th>Address</th>
<th>Protocol</th>
<th>Client-Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>Radius</td>
<td>10.200.206.2</td>
<td>RADIUS</td>
<td>RADIUS Standard</td>
</tr>
</tbody>
</table>
4. Add new access policy. Follow these steps:

Welcome to the New Remote Access Policy Wizard

This wizard helps you set up a remote access policy, which is a set of conditions that determine which connection requests are granted access by this server.

To continue, click Next.

Policy Configuration Method

The wizard can create a typical policy, or you can create a custom policy.

How do you want to set up this policy?

- Use the wizard to set up a typical policy for a common scenario
- Set up a custom policy

Type a name that describes this policy.

Policy name: aruba-policy

Example: Authenticate all VPN connections.
New Remote Access Policy Wizard

Access Method
Policy conditions are based on the method used to gain access to the network.

Select the method of access for which you want to create a policy.

- **VPN**
  Use for all VPN connections. To create a policy for a specific VPN type, go back to the previous page, and select Set up a custom policy.

- **Dial-up**
  Use for dial-up connections that use a traditional phone line or an Integrated Services Digital Network (ISDN) line.

- **Wireless**
  Use for wireless LAN connections only.

- **Ethernet**
  Use for Ethernet connections, such as connections that use a switch.

New Remote Access Policy Wizard

User or Group Access
You can grant access to individual users, or you can grant access to selected groups.

Grant access based on the following:

- **User**
  User access permissions are specified in the user account.

- **Group**
  Individual user permissions override group permissions.

Group name:

Add... Remove
EAP uses different types of security devices to authenticate users.

Select the EAP type for this policy.

Type:

- Protected EAP (PEAP)

Certificate issued: 888-dc-01.kppddp.pajak.go.id

Friendly name:

Issuer: KPPDDP-CA

Expiration date: 12/8/2008 7:07:50 PM

Enable Fast Reconnect

EAP Types

- Secured password (EAP-MSCHAP v2)

Add | Edit | Remove | OK | Cancel
Completing the New Remote Access Policy Wizard

You have successfully completed the New Remote Access Policy Wizard. You created the following policy:

aruba-policy

Conditions:
- NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11"

Authentication: EAP(Protected EAP (PEAP))

Encryption: Basic, Strong, Strongest, No encryption

To close this wizard, click Finish.
5. Edit properties a new access policy that you just created. Follow these steps:

**aruba-policy Properties**

Specify the conditions that connection requests must match.

**Policy conditions:**

- **NAS-Port-Type matches "Wireless - Other OR Wireless - IEEE 802.11"**

If connection requests match the conditions specified in this policy, the associated profile will be applied to the connection.

**Edit Profile...**

Unless individual access permissions are specified in the user profile, this policy controls access to the network.

If a connection request matches the specified conditions:

- [ ] **Deny remote access permission**
- [x] **Grant remote access permission**
6. IAS has been configured.
7. Go to active directory users and components
8. Edit properties wireless user (employee). Follow this step:
Add Radius Server In Aruba Controller

1. Add radius server. Follow this steps: