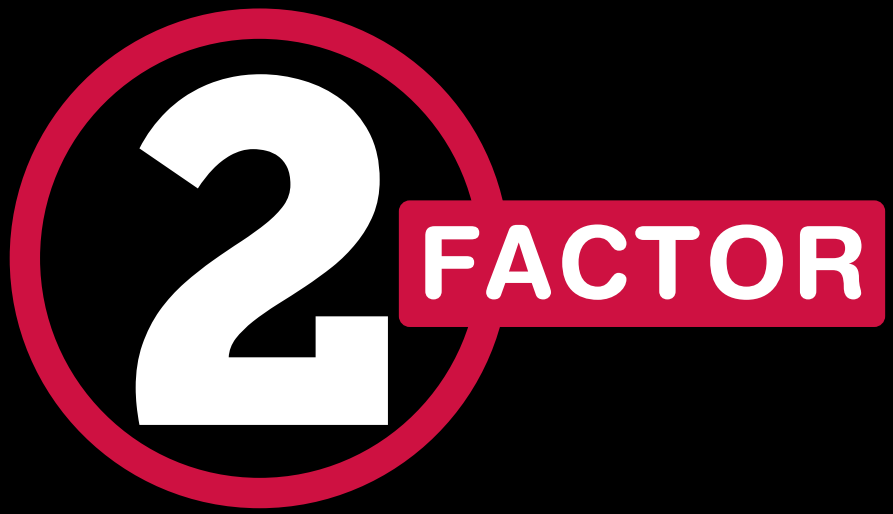


E-Guide to adding Two-Factor Authentication to your Corporate Network

IRC: # wikid on freenode.net
@wikidsystems

www.wikidsystems.com

Contents

Overview

Static passwords are showing their age. As more and more users sign up for more and more Internet services, password reuse is major problem. The adoption of cloud services by companies means that a username and password is often the only thing protecting key data. More and more companies are under regulator compliance and are required to implement stronger security measures such as two-factor authentication.

In addition, the data shows that attackers routinely take advantage of weaknesses in authentication. According to the 2012 Verizon Data Breach Investigation Report (http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2012_en_xg.pdf) 5 out of 10 threat actions involved authentication as well as 4 of the 5 top hack methods.

At WiKID, we applaud the increasing adoption of two-factor authentication. Our goal has always been to make two-factor authentication less expensive, easier to implement and easier for the end-user. We have an open-source version of our product and we have produced extensive documentation on how to add two-factor authentication to a number of commercial products and open-source projects.

This e-book is our attempt to summarize how to add two-factor authentication into your network as easily and securely as possible. While we use WiKID as the authentication server, this document applies no matter what authentication system you use. We will use standard protocols and popular systems for examples. Most of our deployments use exactly this configuration, with minor changes.

So, this is another gift from WiKID to the community. We hope that it helps increase your security.

Terms

Access Client – The user's device or VPN client.

Network Access Server – AKA a RADIUS client, A Network Access Device (NAD), remote access server (RAS), is a VNP or Access point processes an authentication request from an access client. We use the term Radius client.

Radius Server – processes authentication and authorization requests and performs accounting. These functions may be forwarded to a separate server or service such as AD, OpenLDAP or the WiKID server.

Authentication Server – A back-end server that performs authentication as requested by the RADIUS server.

Directory Server – a database of users and roles, such as an LDAP server or Active Directory

Audience

This guide is designed for Enterprise-oriented information security practitioners and systems administrators. Typically, our customers have a directory in place, mostly AD, though a good number have OpenLDAP. While most have an Enterprise-class VPN from the likes of Cisco or Juniper, many have OpenVPN or pfsense. The configuration laid out here will work with all those – even high-end Netgear boxes can be configured in this setup.

We often get asked "Does WiKID work with VPN X?" This guide seeks to answer our most frequent questions. After reading this guide, you should have a clear understanding of how best to configure two-factor authentication in your network.

VPNs

In the simplest configuration a VPN might have a database of users and passwords. The problem with this set up is that you probably also have a directory with users in it, such as Active Directory.

When a user leaves the company, they need to be disabled in both the VPN and AD. This might not be a problem at first, but as companies grow, it becomes a big problem.

1

User enters username and password into VPN

VPN validates user and grants access

This configuration may rely on the VPN's built-in database of users and passwords.

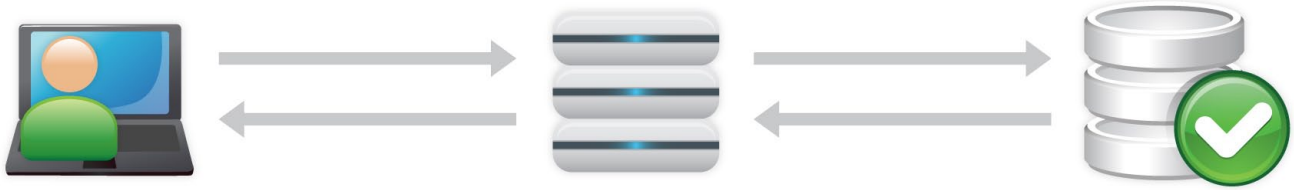
VPNs

Obviously, a much better way is to have the directory perform authorization and authentication against its existing database. All enterprise/business level VPNs can do this.

They can do this via "Active Directory Integration" or LDAP. They can all do it via RADIUS too.

Turns out that RADIUS is the best option.

2

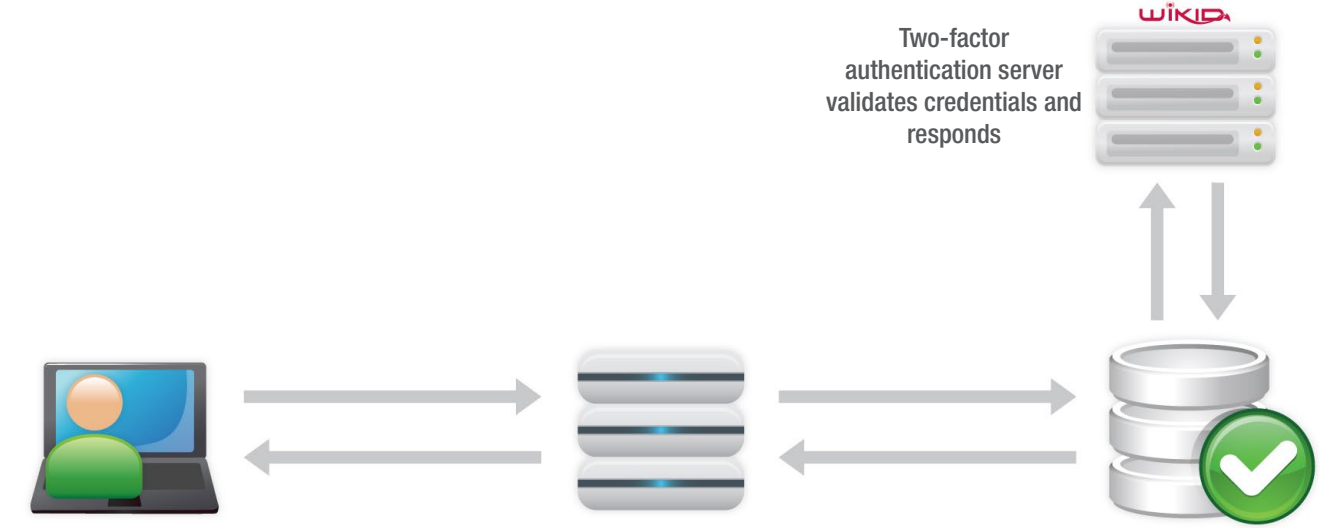


This configuration uses the VPN's built-in support for Active Directory or LDAP.

Separating Authorization and Authentication

Because with RADIUS, Active Directory (and other directories) will proxy the authentication credentials again. This configuration allows you to add two-factor authentication to your network easily. Oh, and your directory will still do authorization so disabling a user there will prevent them from logging in.

1

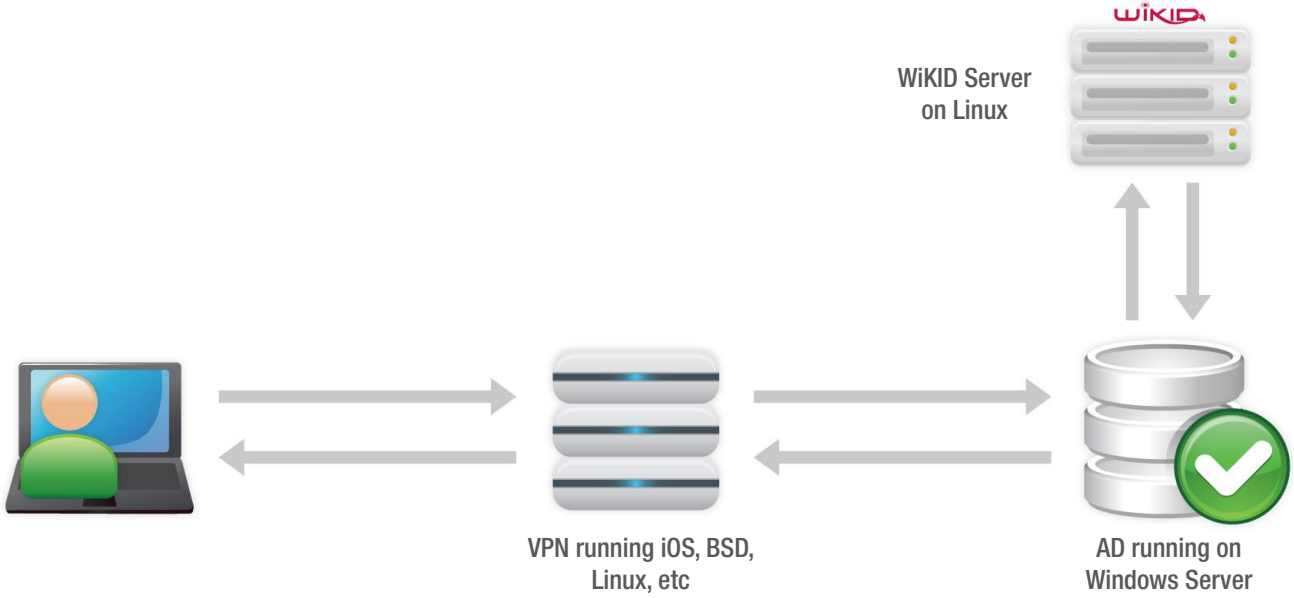


SHARE THIS eBOOK

Separating Authorization and Authentication

An interesting* side benefit to separating Authorization and Authentication is that you could have a VPN running Cisco iOS, a directory running on Windows and a two-factor authentication server running Linux all working together.

2



Access to the WiKIDAdmin can be more limited since users can be disabled in AD.

AD Admins can disable a user here and lock them out entirely.

*** Well, interesting to me.**

SHARE THIS eBOOK

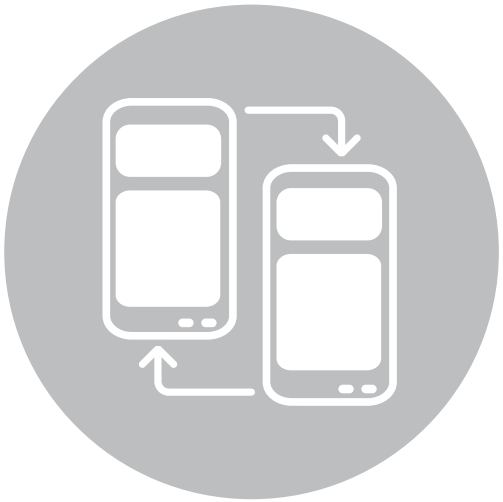
Radius Clients

A Radius client sends authentication credentials to a Radius server, which might respond or might proxy the credentials to another server.

The minimum information needed is the IP Address of the Radius server, the port used (1812 is the default) and a shared secret used to encode the traffic.

Note that depending on the flavor of radius used, traffic may only encoded, not encrypted, so encryption must be added if you're using an untrusted network.

We'll be doing a three example clients, a Cisco VPN, a Juniper VPN and an SSH client.



Cisco Example

1. From the Concentrator Manager, select Configuration → System → Servers → Authentication click Add and enter: Server Type: RADIUS

2. Authentication Server: Hostname or IP address of the WiKID Strong Authentication Server

3. For Server Port, enter 1812

4. For the Server Secret. enter a shared secret that you will later set in the WiKID server.

5. Under Configuration → User, Create a group and set its Authentication Type RADIUS. Give the group a name and a password. Since you are configuring this group on the VPN3000, select type to be Internal.

6. The Web VPN uses the first authentication server listed in the Authentication Server list to authenticate all users. Go to Configuration → System → Servers → Authentication and move the new radius authentication server to the top.

7. Change the Login Message displayed to the user by going to Configuration → Tunnel and Security → WebVPN → Home Page. Then enter the Login Message, such as "Please enter your username and WiKID Passcode."

Juniper Example

1. Go to Auth Servers.
2. From the New: dropdown menu, select RADIUS Server, and click New Server...
3. Name the new RADIUS server WiKID-Test-RADIUS-Server.
4. Verify that the NAS-Identifier field is populated with the hostname of your IC. If not, enter the hostname in that field. (Populated from Network → Overview → Hostname field.)
5. In the RADIUS Server: field, enter the IP address of the WiKID RADIUS server.
6. Verify that the authentication and accounting ports are set to 1812/1813.
7. In the Shared Secret: field, enter the RADIUS secret.
8. If your IC is behind a NAT, enter the external address of the NAT in the NAS-IP-Address field. If your IC is not behind a NAT, leave this field blank.
9. Click Save Changes.
10. Go to Auth Servers and verify that the RADIUS server instance was created successfully.

Juniper Example continued

1. Go to User Roles → New User Role...
2. Name the new role WiKID-Test-Role, then click Save Changes.
3. Go to User Roles and verify that the new role was created successfully.
4. Go to User Roles → WiKID-Test-Role → Agent → General. Uncheck Install Agent for this role, then click Save Changes.
5. Go to User Roles → WiKID-Test-Role → Agentless. Check Enable Agentless Access for this role, then click Save Changes.

Juniper Example continued

1. Go to User Realms → New User Realm...
2. Name the new realm (for example WiKID-Test-Realm).
3. From the Authentication: dropdown menu, select WiKID-Test-RADIUS-Server.
4. Click Save Changes.
5. Go to User Realms → WiKID-Test-Realm → Role Mapping, and click New Rule...
6. Verify that the Role Based On: dropdown menu is set to Username.
7. In the Name: field, enter a rule name (e.g. Allow-All-Users).
8. Under Rule: If username..., verify that the dropdown menu is set to is, then enter * in the username field.
9. From the Available Roles list, select WiKID-Test-Role, then click Add to move it to the Selected Roles list.
10. Click Save Changes, and verify that the new rule was created successfully.

Pam Radius

PAM stands for Pluggable Authentication Module. It is the standard authentication mechanism in Linux. PAM handles authentication and authorization.

PAM can be confusing and it is different across Linux flavors. But many, many programs support it, so once you understand how it works and configure it, you can easily add services to it.

SSH, OpenVPN, Postgresql, sudo, login, FreeNX, etc, all support PAM authentication.

Pam Radius Example

1. Download pam_radius

2. Untar, run 'make'

3. Copy resulting shared lib:
   sudo cp pam_radius_auth.so /lib/security/

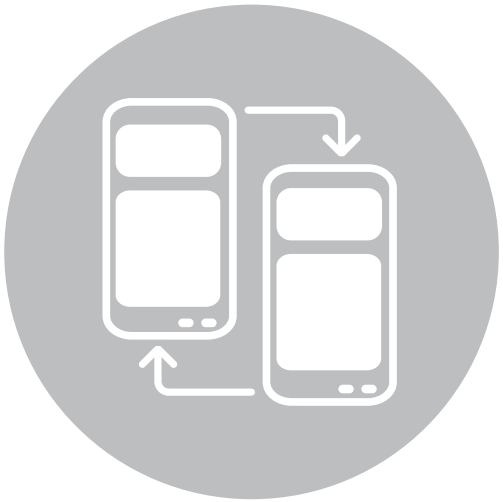
4. Edit /etc/pam.d/sshd to allow Radius authentication:
   auth sufficient /lib/security/pam_radius_auth.so

5. Edit or create your /etc/raddb/server file adding this line:
   routableIPaddress shared_secret 1

Network Clients

Needless to say, we can't include every VPN as an example in this eGuide. We have a number of tutorials on our website (www.wikidsystems.com/support/wikid-support-center/how-to), many contributed by our users. The Apache integration tutorials may be particularly useful.

If you have a custom application that doesn't support Radius, we also have an API and supporting packages in Java, Python, Ruby, PHP and C# (www.wikidsystems.com/downloads/network-clients). The API can be used to create simple applications to register users as well – securely and even across different enterprises.



Directory Integration

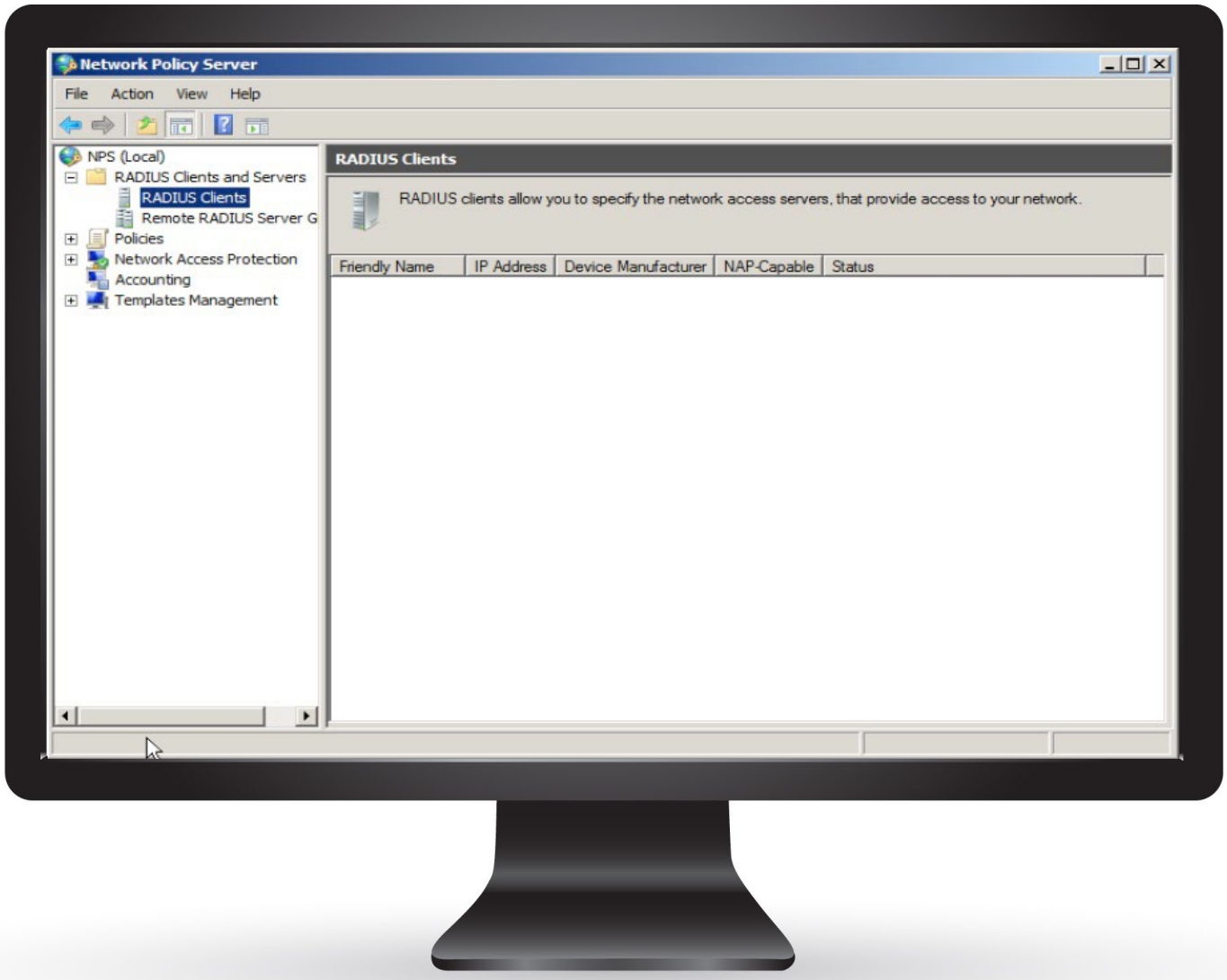
Now that we've configured the Network Clients, let's get them talking to our Directory.

We'll be integrating Active Directory into the process using the Microsoft radius plugin, Network Policy Server or NPS. The directory will be authorizing the users' access and then proxying the credentials to the WiKID two-factor authentication server for authentication.

A key security benefit is that the user will enter their AD username and the one-time passcode into their VPN client. Hopefully, they will only use their AD password on the LAN.

Active Directory

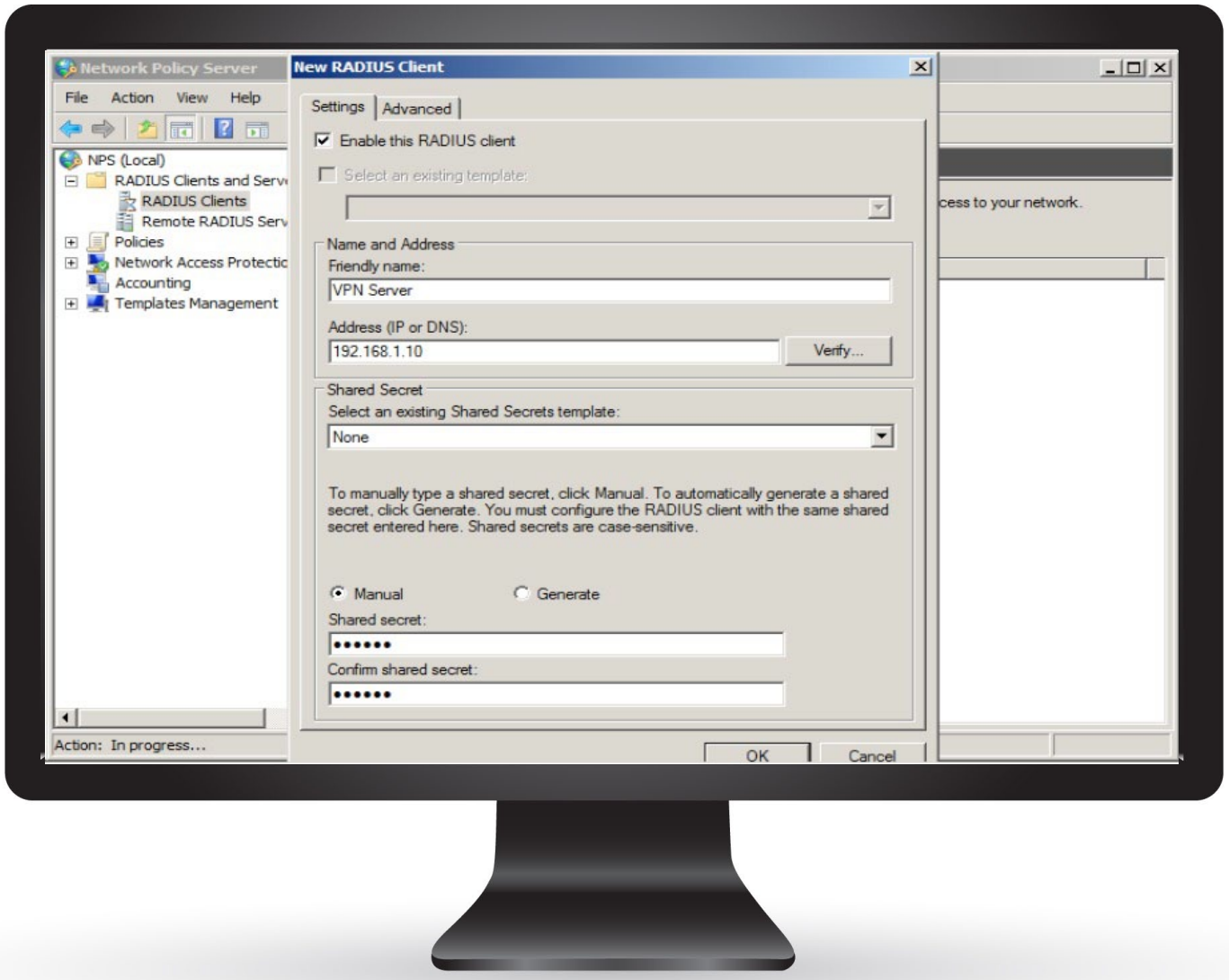
Add the Network Policy Server role and start the admin tool



SHARE THIS eBOOK

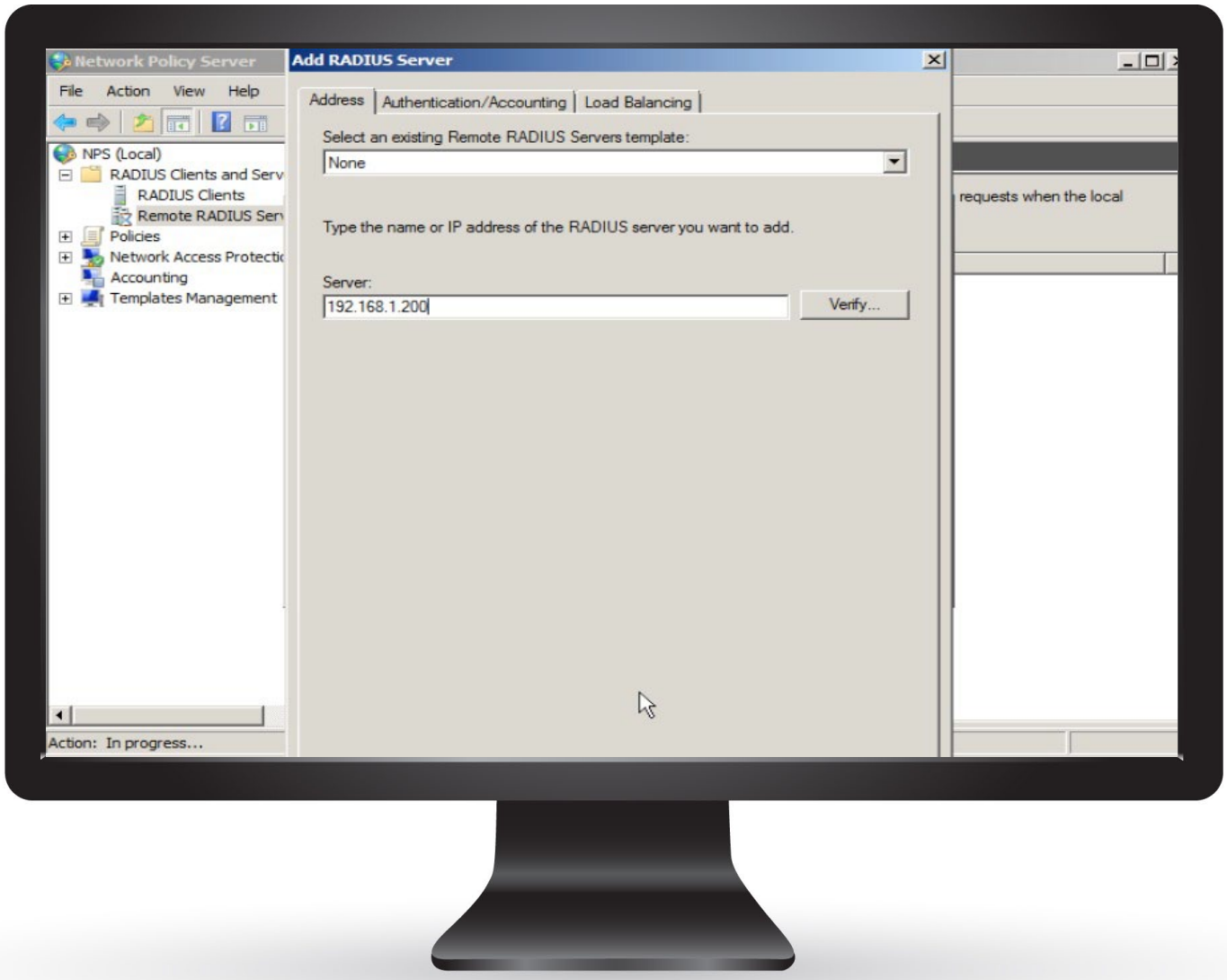
NPS - Add Radius Client

Add a new radius client, entering your VPN's IP address and the shared secret you created



Add WiKID as a Radius Server

Next, right-click on Remote RADIUS Servers and select New. Under Server, enter the IP address of the WiKID Server. Under Authenication/ Accounting, enter the shared secret

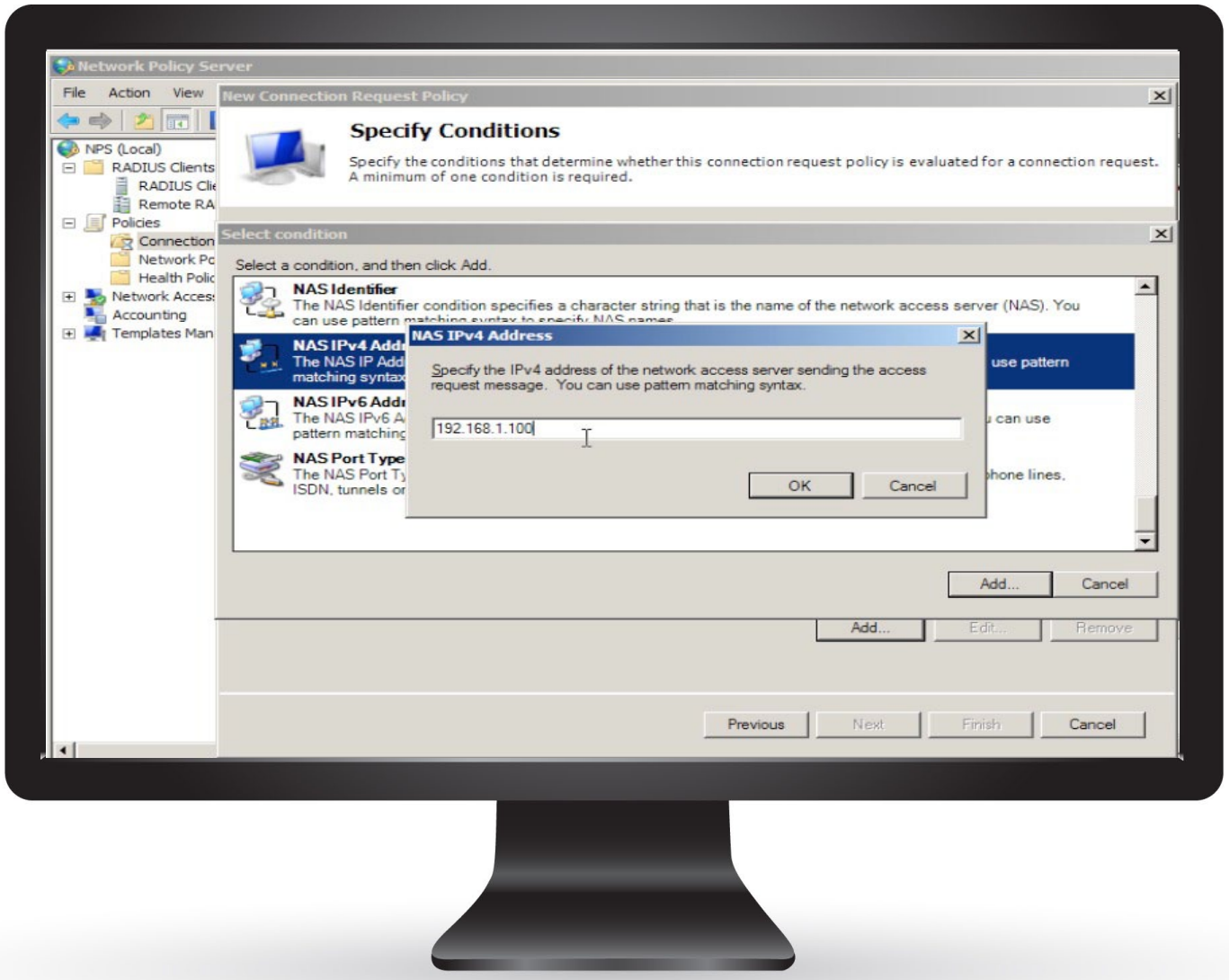


NPS – Add a Condition

You need to add a condition or the policy will never be used. If you want all the users of this RADIUS client to use two-factor authentication, then you can specify that the NASIPv4Address of the VPN be used. You can also state that connections at any time use two-factor authentication. You can also limit it to certain users. Please see the Microsoft documentation for more details.

NPS - NAS IP

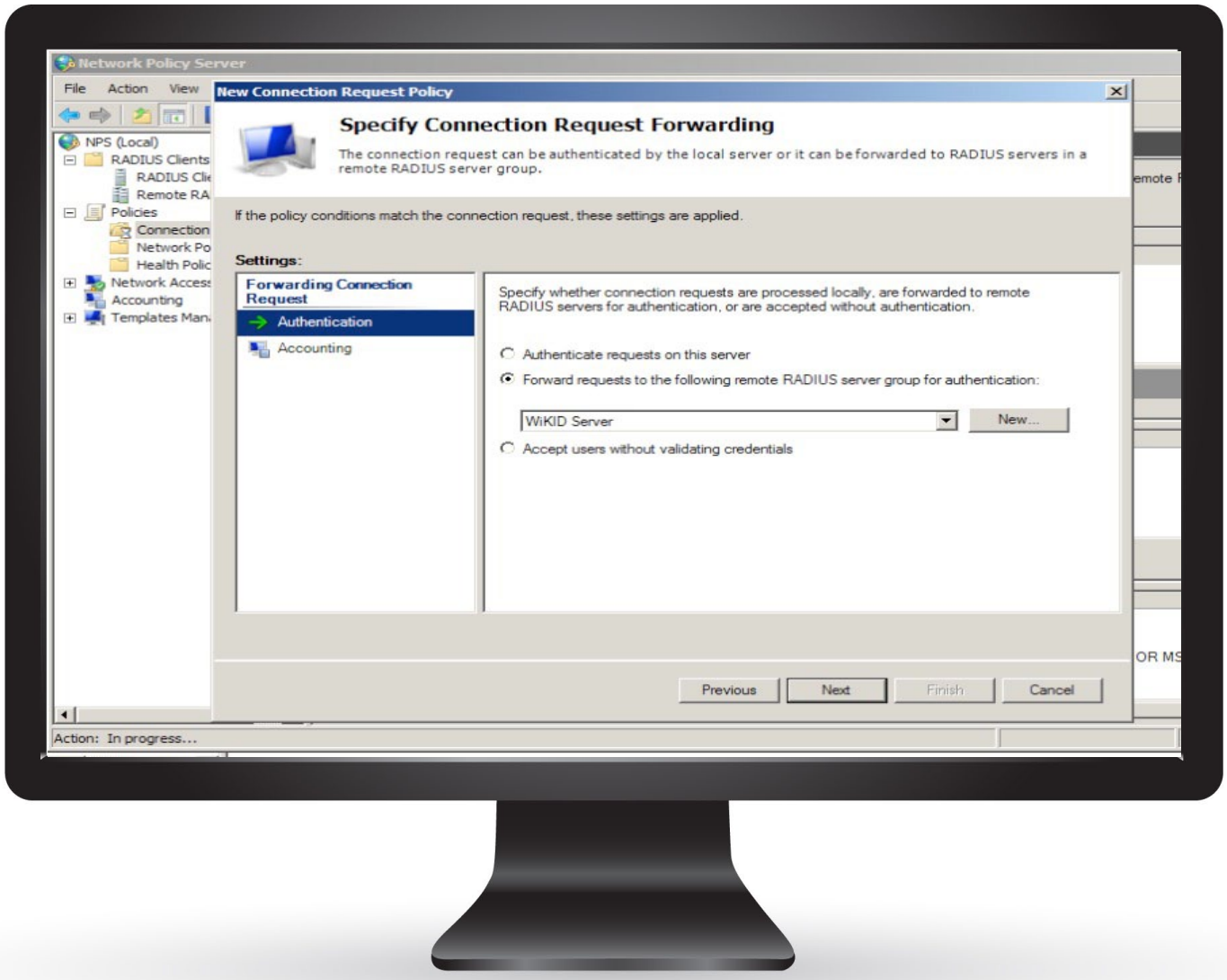
Create a new Connection Policy and choose your condition. We use the NAS IP, which is your VPN IP address.



SHARE THIS eBOOK

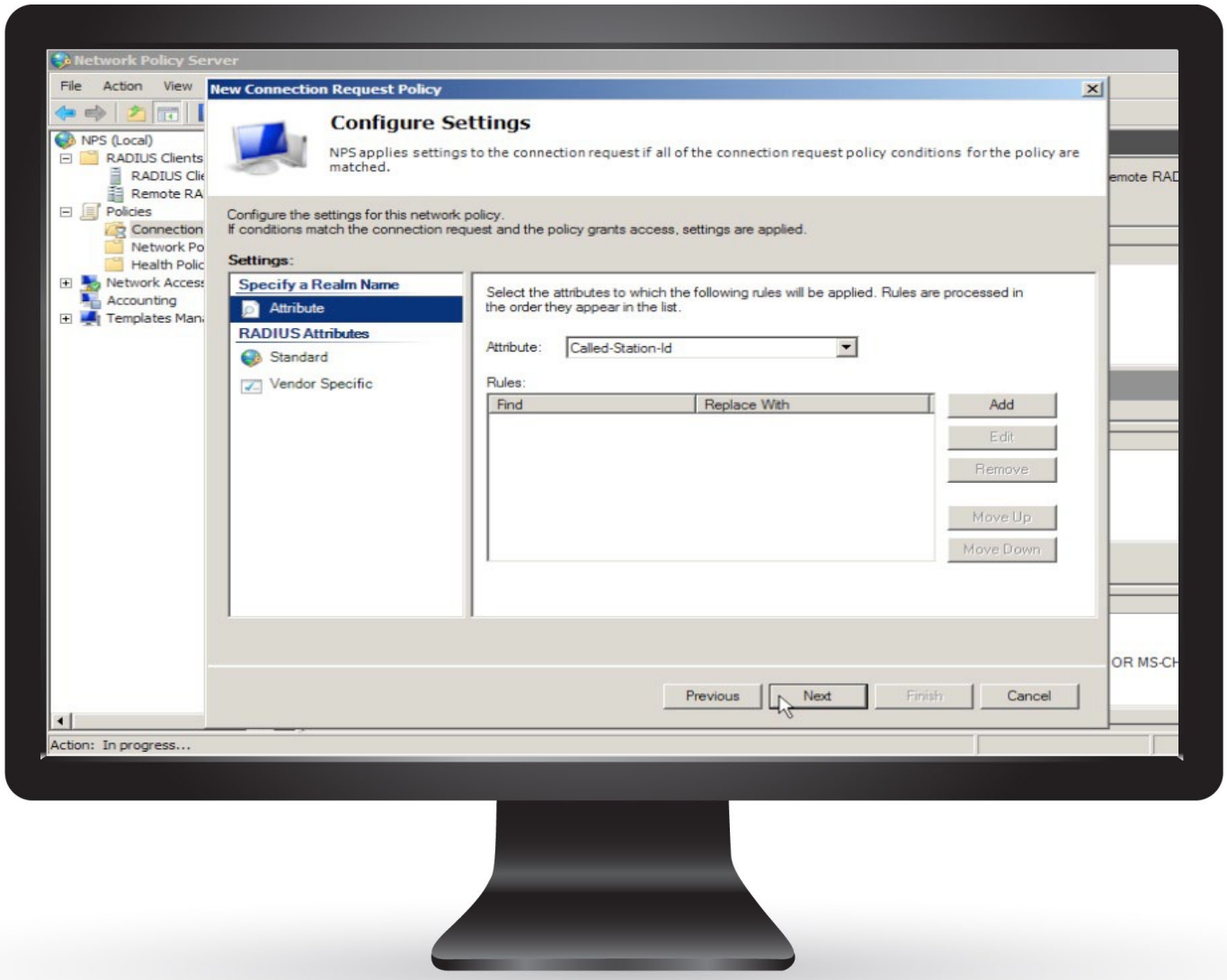
NPS

Click Next and select Authentication. Choose the radio button to forward requests and select the WiKID server.



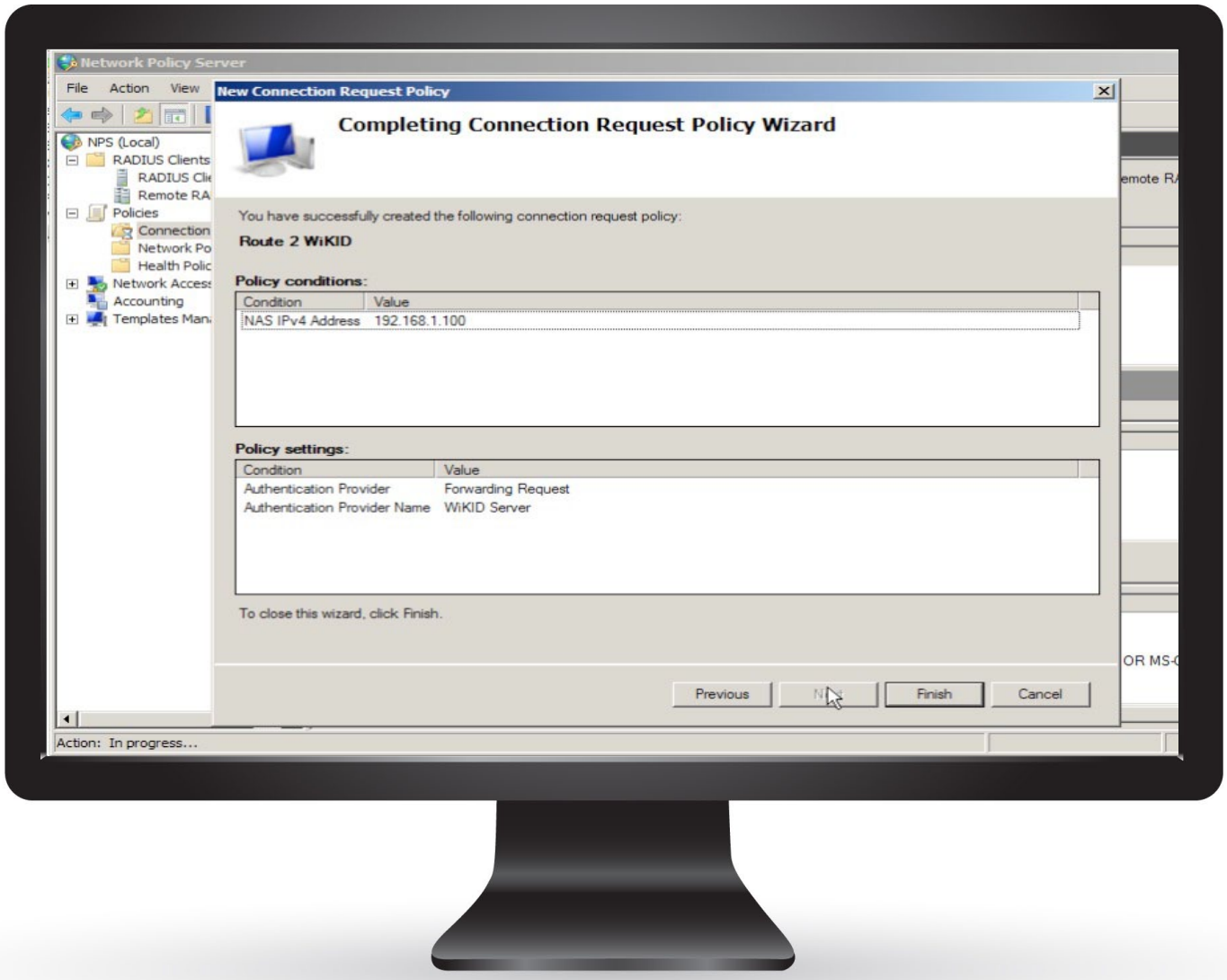
NPS – Radius Attributes

Click next. Do not specify any RADIUS Return Attributes. Attributes are outside the purview of this e-guide.



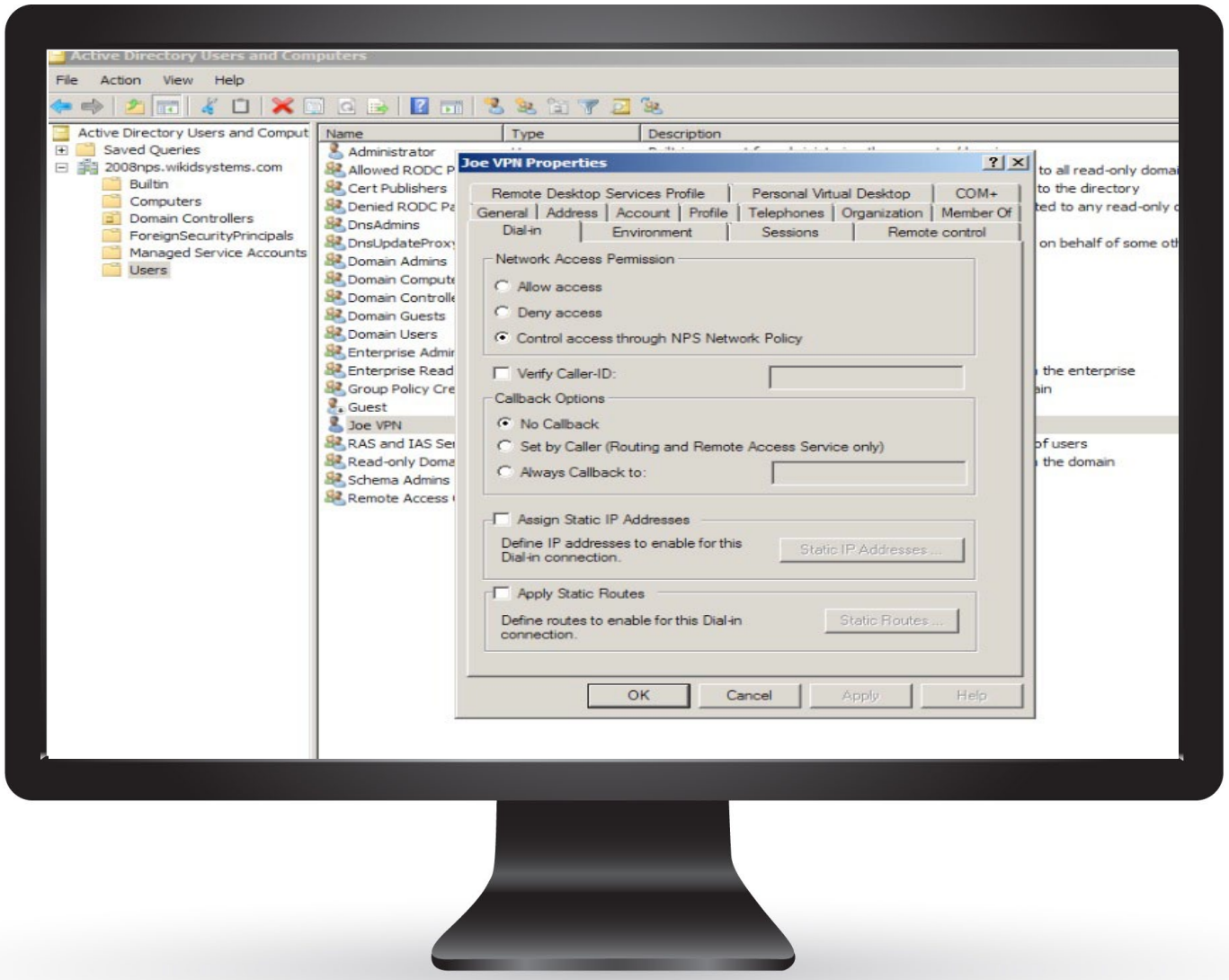
NPS

Click Finish and review the settings.



NPS – Adding Dial-in Permissions

In the AD Users and Computers admin tool and click on Users. Click on the user's Dial-in tab. Under Network Access Permission, choose Control Access through NPS Network Policy.



SHARE THIS eBOOK

Adding Two-Factor

The final step of the configuration is to have the two-factor authentication server perform the authentication.

Remember, the user has entered their AD username and the one-time passcode. NPS performs authorization based on the username and conditions. It will then proxy the credentials to the WiKID server for authentication.

In addition to not using a LAN password outside of the LAN, security is increased by separating Authorization and Authentication. Now, an AD admin or HR person can disable a user's remote access in AD without having access to the WiKID server.

In addition, it is now quite simple to add more Radius clients into this setup. Each of our examples, the Cisco, the Juniper and the SSH serer can easily route your logins through AD and Radius.

Configuring WiKID

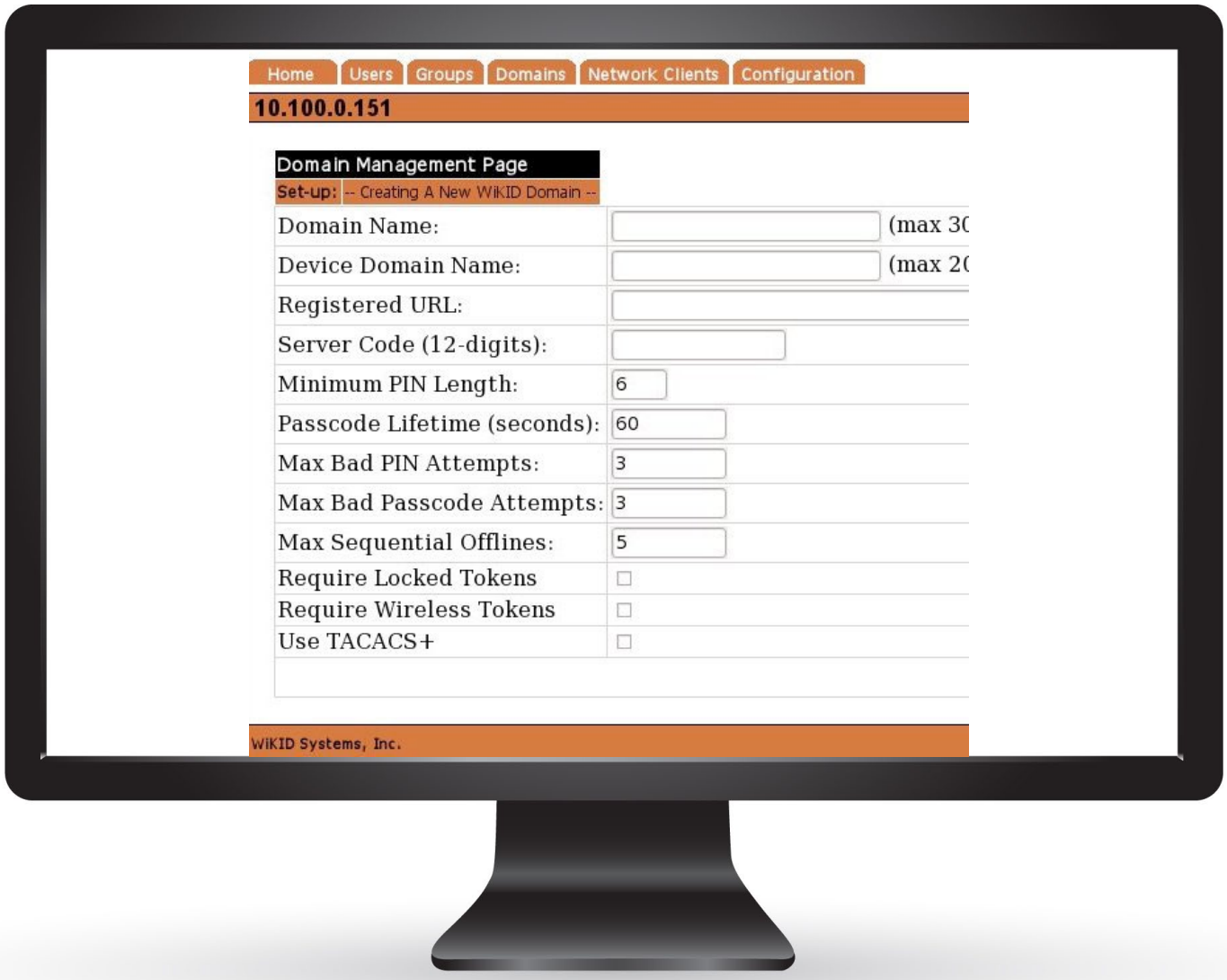
We are assuming you have already configured your WiKID server. We will just be adding a domain, configuring a network client.

In WiKID, users are associated with Domains. Domains are in turn associated with Network clients. In this example, the Network Client will use the Radius protocol. Other supported protocols include LDAP, TACACS+, GoogleSSO and our own protocol wAuth.

Download a free trial of the WiKID Strong Authentication Server

WiKID – Create a Domain

In the WiKIDAdmin UI, click on Domains, then add a domain.



WiKID – Domain Configuration

Here are descriptions for the Domain Fields:

Domain Name - This is a descriptive label for this domain visible only in the administration system.

Device Domain Name - This is the domain label that will appear in the menu option on the client device. This label should be relatively short to facilitate viewing on a mobile device.

Registered URL - Enter an HTTPS URL here if you want this domain to support mutual authentication. In brief, the WiKID server will fetch the certificate and store a hash of it. When a user requests a one-time password from a PC software token, the token client will also get this hash and URL. Before presenting the one-time password, it will fetch the URL's certificate, hash it and compare the two. If the hashes match, the OTP will be presented and the default browser (if supported) will be launched to the URL. This system will prevent network-based man-in-the-middle attacks. Leave this empty for non-SSL VPNs.

Minimum PIN Length - This is the minimum allowable PIN length for this domain. Any attempt to set a pin shorter than this value will generate an error on the client device.

Passcode Lifetime - This parameter specifies the maximum lifetime of the one-time passcode generated in this domain. After N elapsed seconds, the one-time passcode will automatically be invalidated.

Server Code or Domain Identifier - This is the zero-padded IP address of the server or the pre-registered prefix in the wikidsystems.net domain. This value must be exactly 12 digits in length.

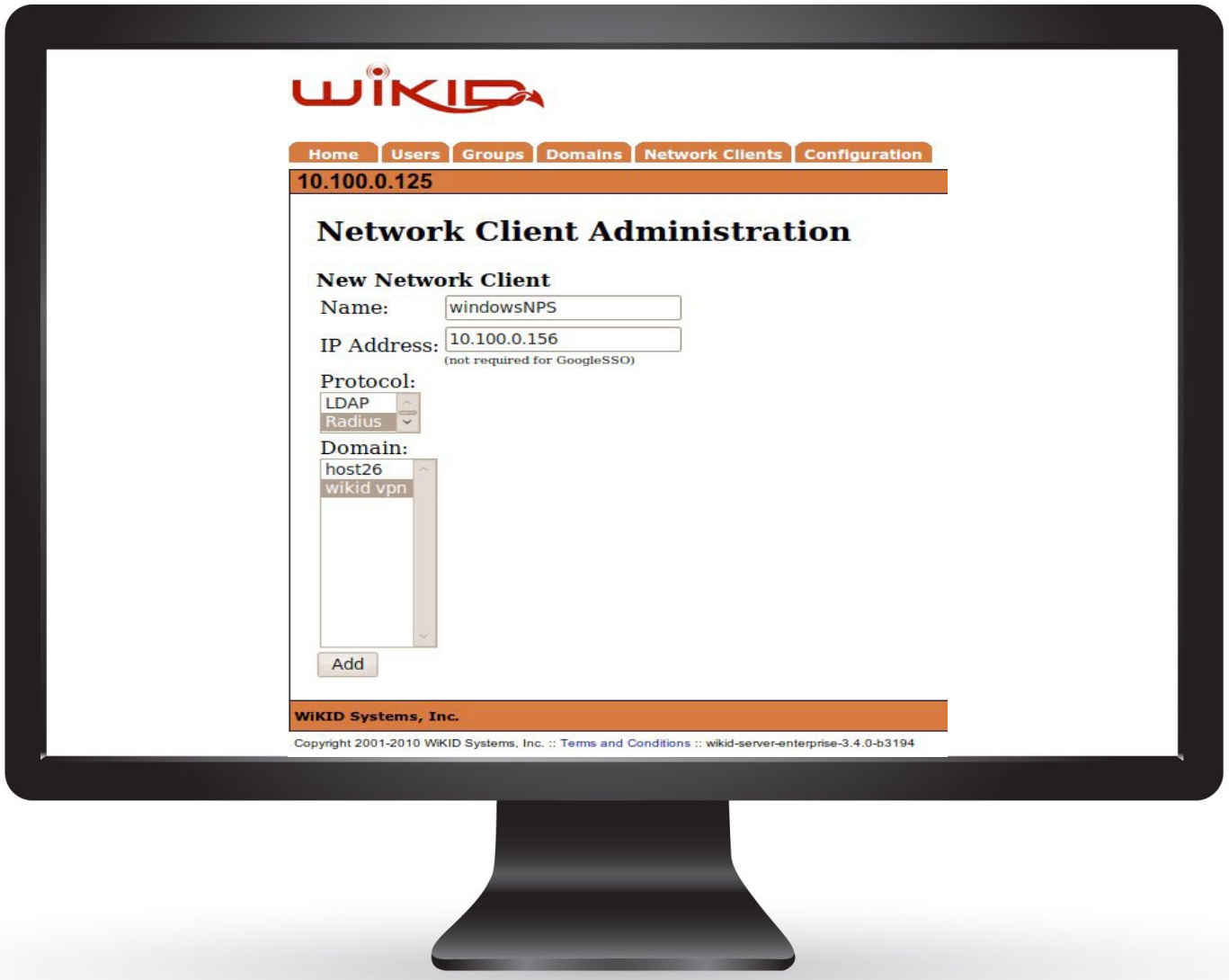
Max Bad PIN Attempts - The maximum number of bad PINs attempted by a device in this domain before the device is disabled.
Max Bad Passcode Attempts - The maximum number of bad passcodes entered for a userid registered in this domain before the userid is disabled.

Max Sequential Offlines - The maximum number of times a device may use the offline challenge/response authentication before being required to authenticate online. This feature is used in the Enterprise version for the wireless clients when they are out-of-network coverage.

Use TACACS+ - Select this to use TACACS+ for this domain.

WiKID – Network Client

Click on the Network Clients Tab and then "Create a New Client". Give it a name and enter the IP Address of your NPS server. Select Radius and specify the correct domain.

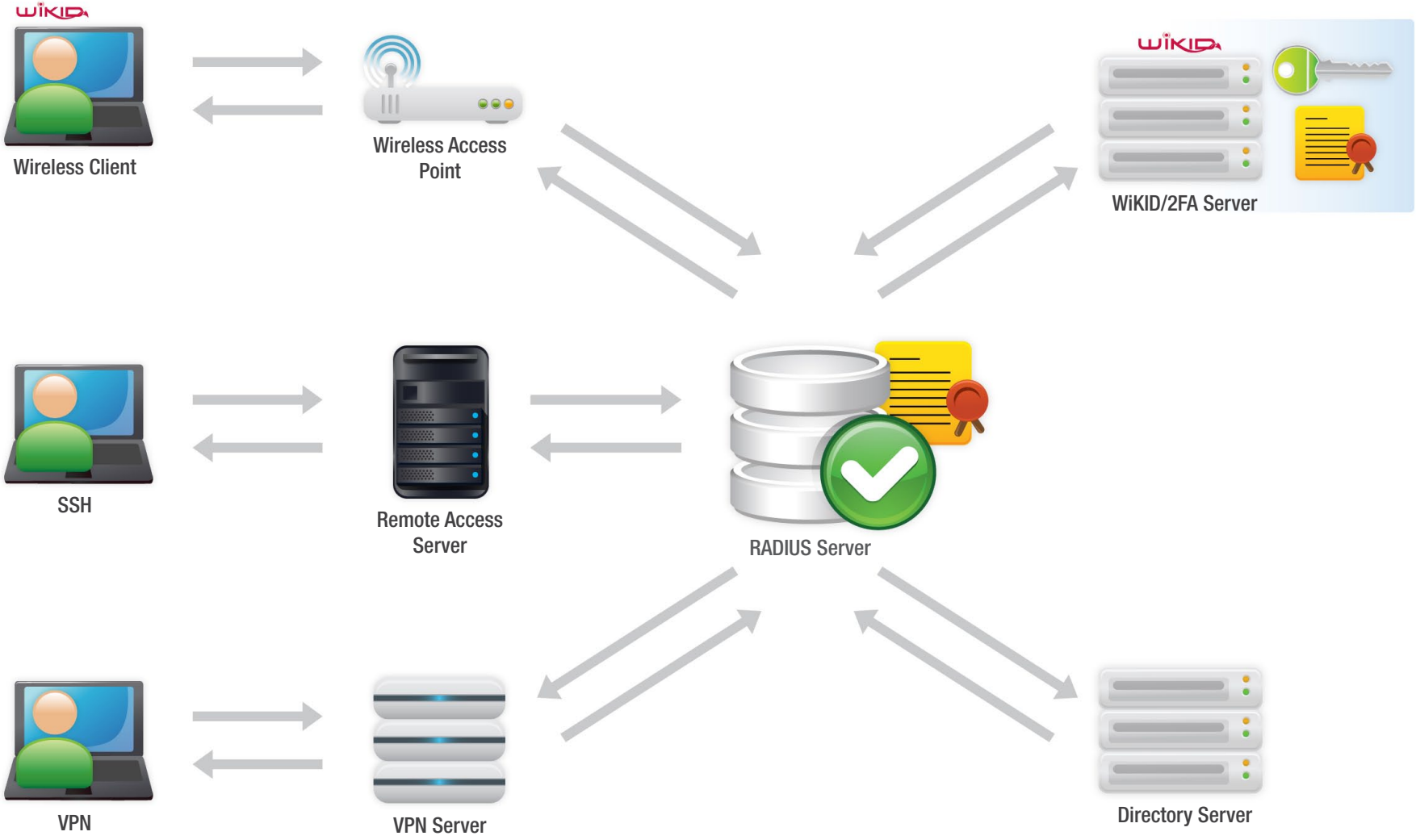


WiKID - Shared Secret

Click Add and then you will be asked to specify a shared secret. Again, leave Return Attributes empty. Restart the WiKID process to load the new radius cache.

That's it. Time to test it.

Two-factor in Your Network



SHARE THIS eBOOK

Summary

Implementing two-factor authentication in your network adds a great deal of security. WiKID has helped hundreds of companies implement two-factor authentication in their network. This eGuide represents how almost all of our customers have deployed WiKID. Integrating your directory in the process

In addition to remote access, you should consider adding two-factor authentication to your critical infrastructure and accounts. For example, the PAM ssh example can be extended to sudo. Logins to your critical switches should be protected as well.

Get Started Today

Whether you are meeting compliance requirements, switching from a more expensive product or just looking to increase your ability to sleep at night, get started today by downloading the WiKID Strong Authentication Server.

www.wikidsystems.com/downloads

It is quick and easy to setup and you maintain control of your server and users. Pricing is simple and posted online – there are no extra charges for support orSMS or telecom fees.

Contact Us

www.wikidsystems.com

IRC: # wikid on freenode.net

Twitter: @wikidsystems

SHARE THIS eBOOK