What is Web Application Proxy?

Web Application Proxy – The Web Application Proxy is a new role service in the Windows Server Remote Access role. It provides the ability to publish access to corporate resources, and enforce multi-factor authentication as well as apply conditional access policies to verify both the user's identity and the device they are using resources, and enforce multi-factor authentication as well as verify the device being used before access is granted.

Web Application Proxy Functionality

The Web Application Proxy (WAP) is a Role Service under the Remote Access role of Windows 2012 which also includes DirectAccess, VPN and routing services. It can provide simple reverse proxy functionality using 'Pass-through' where no preauthentication is performed, or provide Active Directory Federation Services (AD FS or ADFS) authentication by performing the ADFS proxy function. Note that even in Pass-through mode, WAP needs a Windows Server 2012 R2 Preview ADFS farm and must be setup as an ADFS Proxy. Without ADFS you can't even complete the configuration wizard. Pass-through and ADFS federation to claims aware applications can be performed like previous AD FS proxies as a workgroup machine in the DMZ.

Web Application Proxy is a new role service in Windows 2012 R2, that can be configured as an ADFS Proxy or Reverse Proxy solution (an alternative to TMG / UAG) to publish applications to the internet.

Web Application Proxy serves as a barrier between the Internet and your corporate applications. In many organizations, when you deploy Web Application Proxy and publish applications through it, those applications will be available to external users on devices that are not joined to your domain; for example, personal laptops, tablets, or smartphones. These devices are not domain-joined and as such, they are described as unmanaged devices, and are untrusted within the corporate network. Since you want your users to be able to access important information whenever and wherever they are located, you must mitigate the security risk of allowing users access to corporate resources from these unmanaged and untrusted devices. Web Application Proxy provides a number of security features to protect your corporate network from external threats. **Web Application Proxy uses AD FS for authentication and authorization to ensure that only users on devices who authenticate and are authorized can access your corporate applications.**

Web Application Proxy must always be deployed with AD FS. This enables you to leverage the features of AD FS, such as, single sign-on (SSO). This enables users to enter their credentials one time and on subsequent occasions, they will not be required to enter their credentials. SSO is supported by Web Application Proxy for backend servers that use claims-based authentication; for example SharePoint claims-based applications, and Integrated Windows authentication using Kerberos constrained delegation. Integrated Windows authentication-based applications can be defined in AD FS as relying party trusts which can define rich authentication and authorization policies that are enforced in requests to the application.

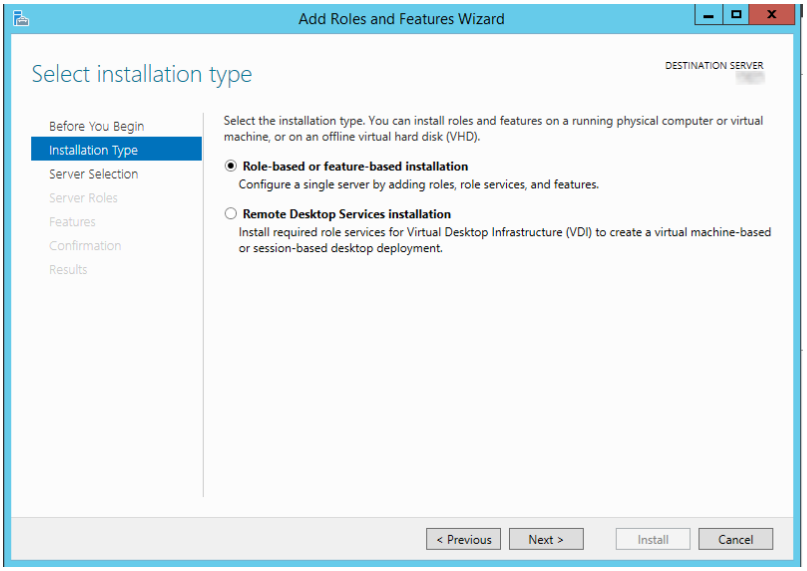
Publishing Application in WAP:

When you publish applications through Web Application Proxy, the process by which users and devices are authenticated before they gain access to applications is known as preauthentication. Web Application Proxy supports two forms of preauthentication:

- AD FS preauthentication—When using AD FS for preauthentication, the user is required to authenticate to the AD FS server before Web Application Proxy redirects the user to the published web application. This ensures that all traffic to your published web applications is authenticated.
- Pass-through preauthentication—Users are not required to enter credentials before they connect to published web applications.

WAP Installation

1. In server manager, click "Manage->Add Roles and Features".
2. Click "Next" on the "Before you begin" screen.
3. For "Installation Type" select "Role-based or feature-based installation" & click "Next".

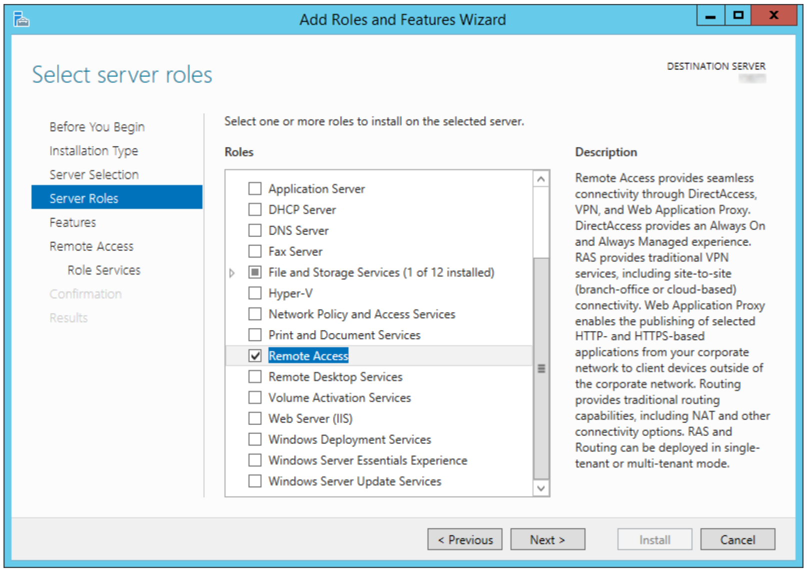


Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

4. Select your desired WAP server and click "Next".
5. On "Add Roles and Features Wizard", select the "Remote Access" role and click "Next".

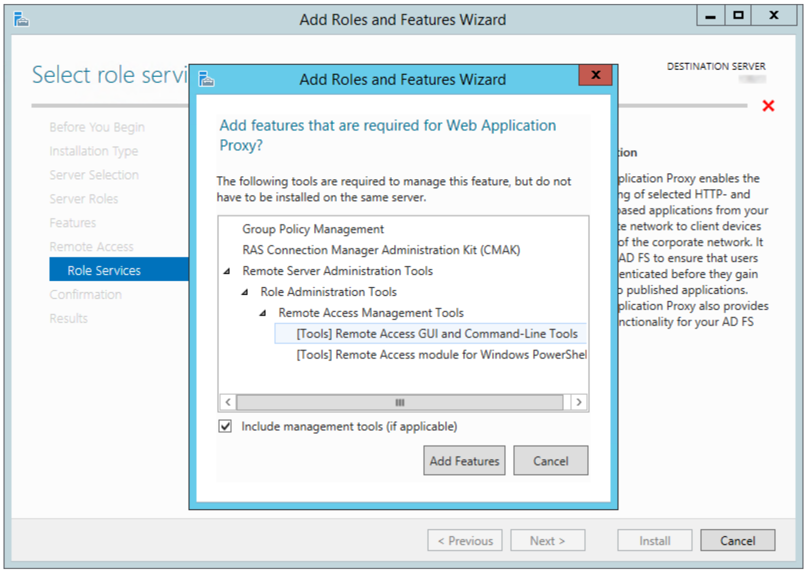


Select one or more roles to install on the selected server.

- ☐ Application Server
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ▣ File and Storage Services (1 of 12 installed)
- ☐ Hyper-V
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☑ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ☐ Web Server (IIS)
- ☐ Windows Deployment Services
- ☐ Windows Server Essentials Experience
- ☐ Windows Server Update Services

Remote Access provides seamless connectivity through DirectAccess, VPN, and Web Application Proxy. DirectAccess provides an Always On and Always Managed experience. RAS provides traditional VPN services, including site-to-site (branch-office or cloud-based) connectivity. Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. Routing provides traditional routing capabilities, including NAT and other connectivity options. RAS and Routing can be deployed in single-tenant or multi-tenant mode.

6. You do not need to select any features; click "Next" on the "Select features" page.
7. Read the dialog presented on the "Remote Access" screen and click "Next".
8. Leave "Include management tools" checked and click "Add Features".



Add features that are required for Web Application Proxy?

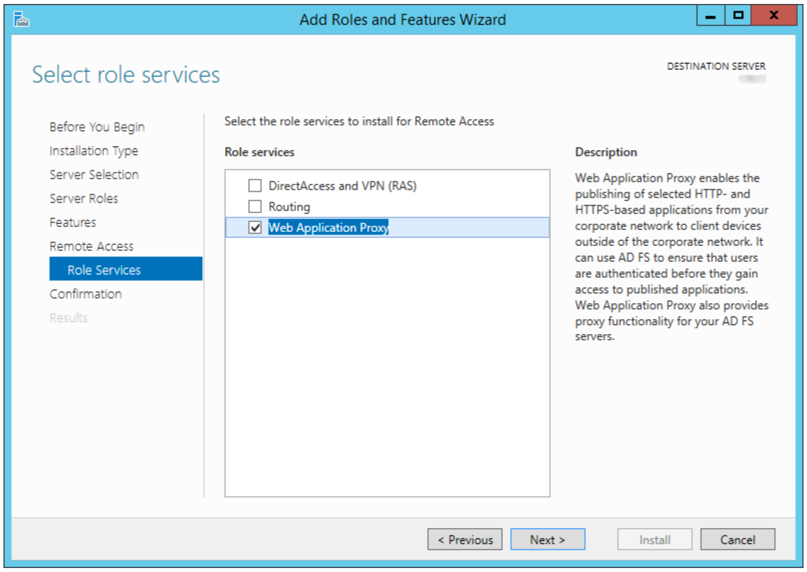
The following tools are required to manage this feature, but do not have to be installed on the same server.

```
Group Policy Management
RAS Connection Manager Administration Kit (CMAK)
◢ Remote Server Administration Tools
    ◢ Role Administration Tools
        ◢ Remote Access Management Tools
            [Tools] Remote Access GUI and Command-Line Tools
            [Tools] Remote Access module for Windows PowerShel
```

☑ Include management tools (if applicable)

plication Proxy enables the ng of selected HTTP- and based applications from your e network to client devices of the corporate network. It AD FS to ensure that users enticated before they gain published applications. plication Proxy also provides nctionality for your AD FS

9. On the "Select role services" page select "Web Application Proxy" and click "Next".



Add Roles and Features Wizard

Select role services

DESTINATION SERVER
[redacted]

Select the role services to install for Remote Access

Role services

- ☐ DirectAccess and VPN (RAS)
- ☐ Routing
- ☑ Web Application Proxy

Description

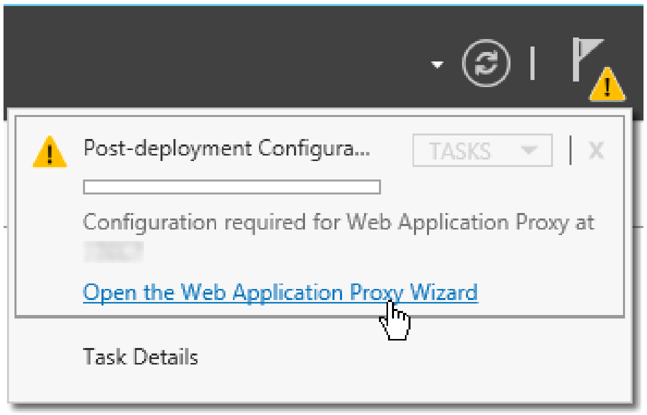
Web Application Proxy enables the publishing of selected HTTP- and HTTPS-based applications from your corporate network to client devices outside of the corporate network. It can use AD FS to ensure that users are authenticated before they gain access to published applications. Web Application Proxy also provides proxy functionality for your AD FS servers.

10. When presented with the confirmation screen, click "Install".

WAP Configuration

Prerequisite Note: For this step you will need the public and private key for your internal ADFS server(s) installed to the "Personal" section of the "Local Computer" store on your WAP server. For more information, refer to "Software Requirements" above.

1. After installation, server manager will notify you that configuration is required. Click the notification flag and select "Open the Web Application Proxy Wizard".



Post-deployment Configura...

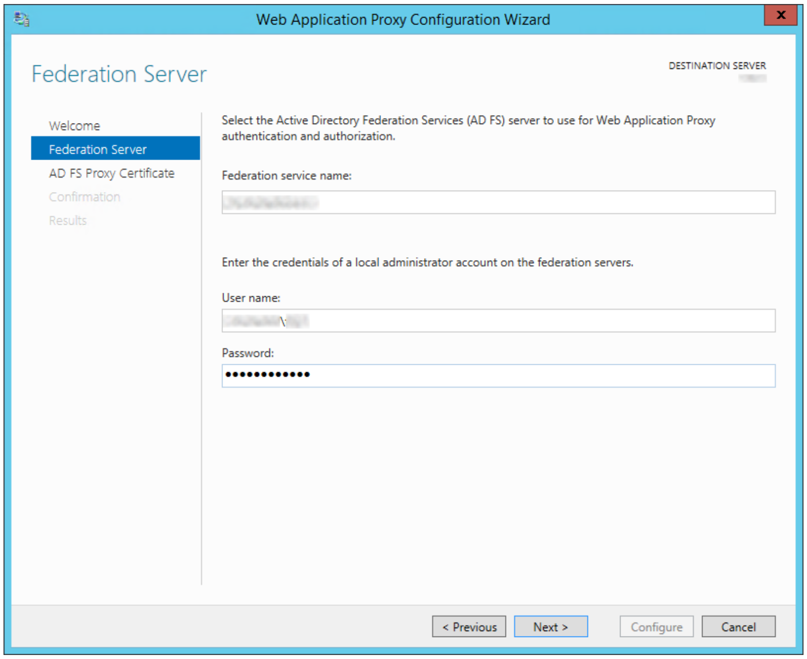
Configuration required for Web Application Proxy at [redacted]

Open the Web Application Proxy Wizard

Task Details

2. On the "Welcome" screen of the "Web Application Proxy Wizard" click "Next".
3. On the "Federation Server" screen, enter the **external** fully qualified domain name of your federation service. This needs to be registered in external DNS (i.e. resolvable from

the internet). For more information, see my article linked under "Software Requirements". Insert the username/password of a domain administrator account to properly register this as a proxy server. This account will **not** be used after this point, so a service account is not necessary. Click "Next".



Select the Active Directory Federation Services (AD FS) server to use for Web Application Proxy authentication and authorization.

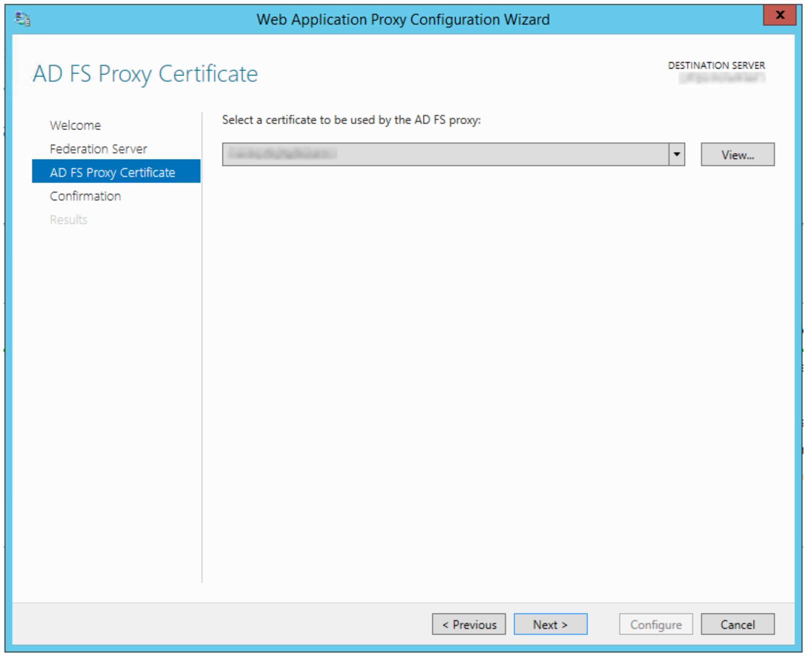
Federation service name: [redacted]

Enter the credentials of a local administrator account on the federation servers.

User name: [redacted]

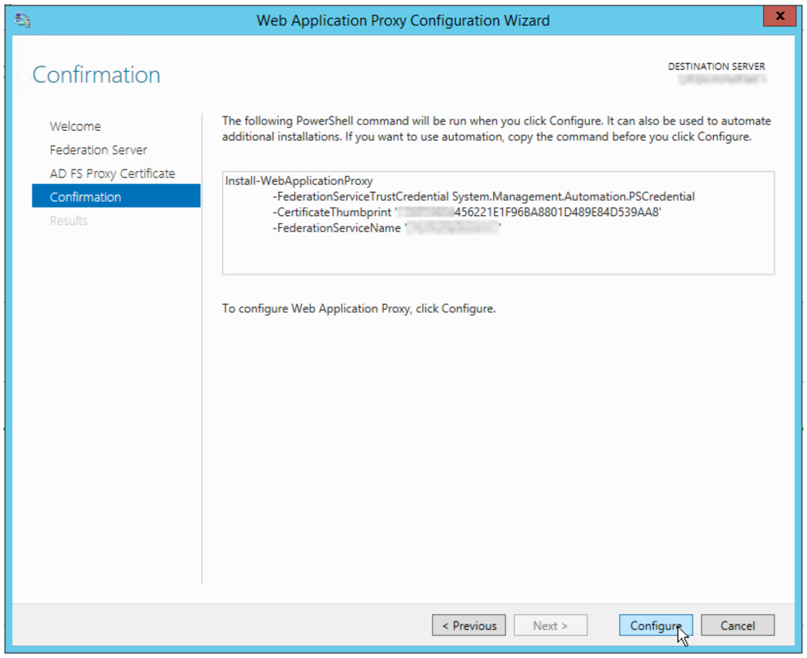
Password: ••••••••••••

4. Select the ADFS certificate you installed earlier from the dropdown and click "Next".



Select a certificate to be used by the AD FS proxy: [redacted]

5. You'll be presented with the configuration details. If you intend on setting up another WAP server for load balancing copy the powershell command down for later use. Click "Configure" to continue.

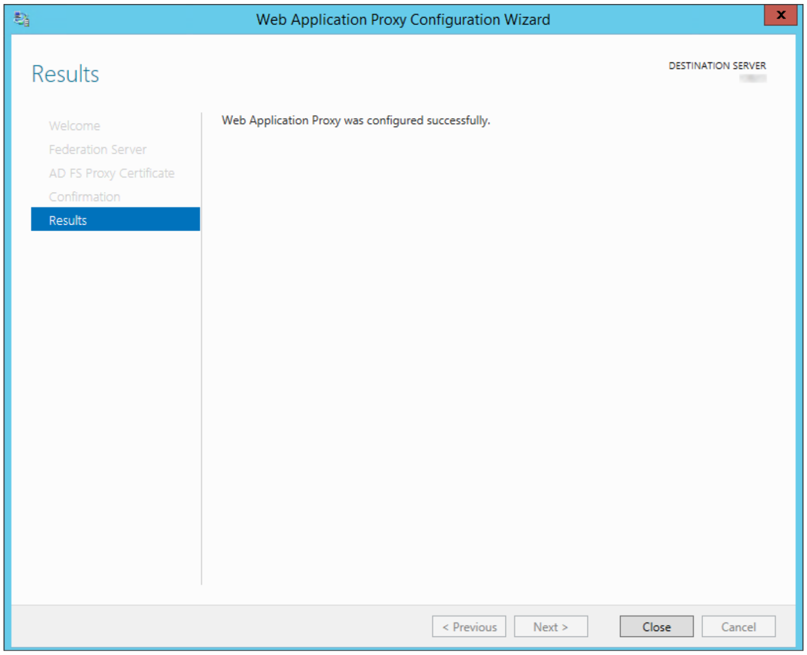


The following PowerShell command will be run when you click Configure. It can also be used to automate additional installations. If you want to use automation, copy the command before you click Configure.

```
Install-WebApplicationProxy
        -FederationServiceTrustCredential System.Management.Automation.PSCredential
        -CertificateThumbprint '[redacted]456221E1F96BA8801D489E84D539AA8'
        -FederationServiceName '[redacted]'
```

To configure Web Application Proxy, click Configure.

6. You should see the message "Web Application Proxy was configured successfully".



Web Application Proxy was configured successfully.

Setup Verification

To verify basic functionality:

1. On the WAP server, open up Tools->Remote Access Management Console
2. On the left-hand navigation pane, select "Operations Status"
3. The status of the WAP server will be relayed in the middle pane. Do not be surprised to see the server listed twice, once for the FQDN and once for netbios. This is normal.