Features - Overview

Simple, Professional and Powerful **Automated Certificate Management**

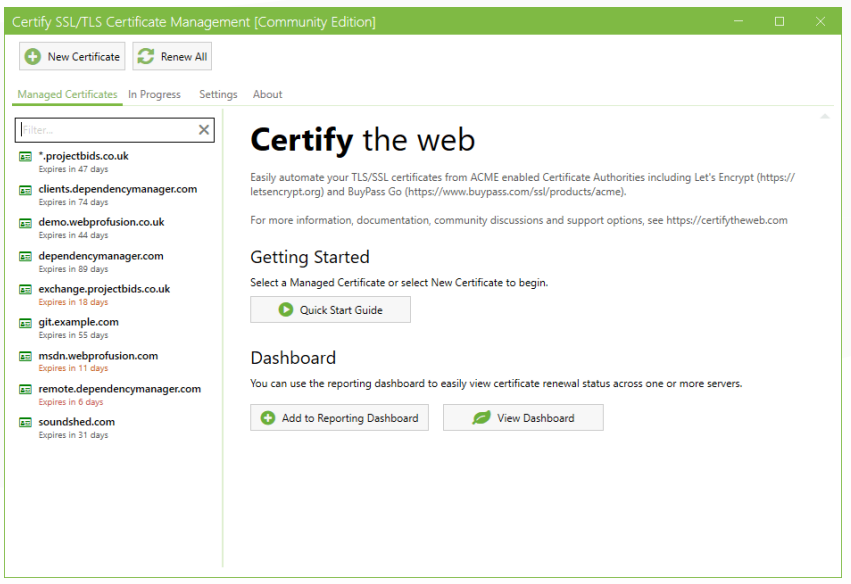
When managing your SSL/TLS certificates for websites, email servers or any other services, you need a simple and reliable automation system with a visual overview that's easy to use and support. As your requirements grow more complex you need a powerful solution that scales, with dedicated support when you need it.

Simply install the app on your server, setup the domains you want to manage certificates for and let the Certify The Web software take care of renewing and (optionally) deploying certificates.

Note: Features described here apply to v5.0 or higher.

Summary

- Easy setup - just install on a supported version of Windows Server.
- Simple certificate requests, authorization, deployment & auto-renewal.
- Ideal for Windows Servers running IIS, but can be used with other services.
- Manage one certificate or several thousand.
- Detailed preview of the certificate request process and planned automated deployment steps.
- Create certificates for single domains, multiple domain (SAN) certificates or wildcard certificates.



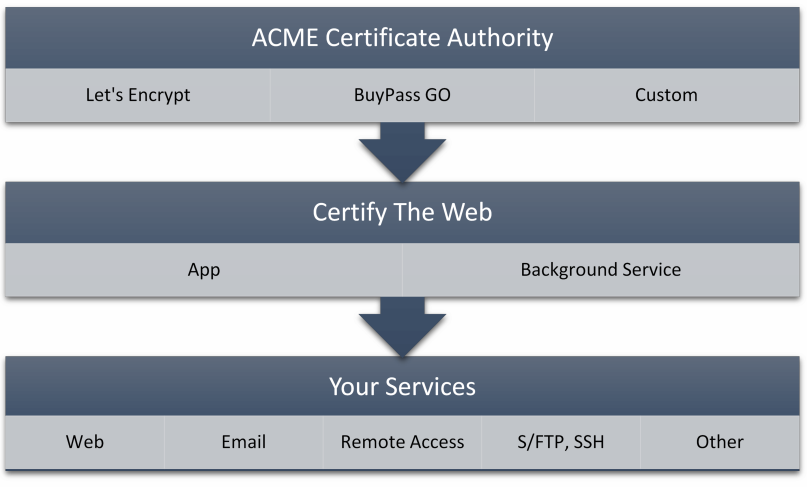
Advanced Features

- Configurable deployment automation.
- Deployment Tasks, for zero-scripting automation of common deployments including:
  - MS Exchange, Remote Access, Remote Desktop Services.
  - Apache, nginx, Tomcat and other services which require PEM or PFX format certificate files.
- Many other advanced features to help your organisation work with your certificates.

How Certificate Automation Works

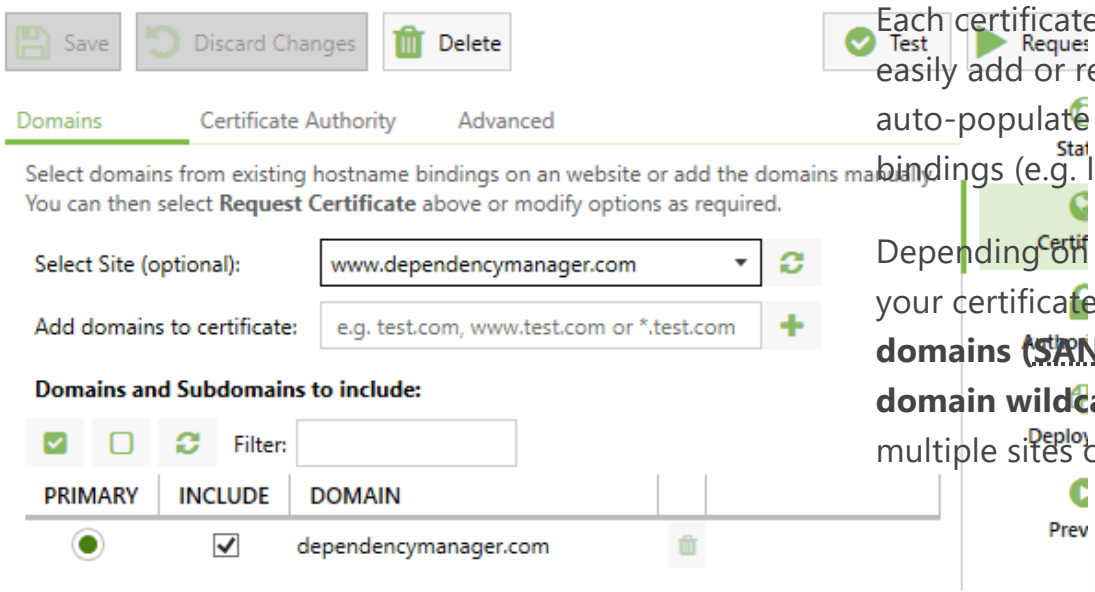
Services which are associated with a domain (websites, mail servers, remote access etc) use DV (Domain Validated) certificates to prove that the service being used is genuine and to encrypt the communication between the end-user and the server itself.

Certificate Automation works by requiring you to regularly prove control of your domains to a Certificate Authority, such as **Let's Encrypt**, who can then issue you a new certificate for your domain with a short expiry date.



Features - Deep Dive

Manage Certificate Domains



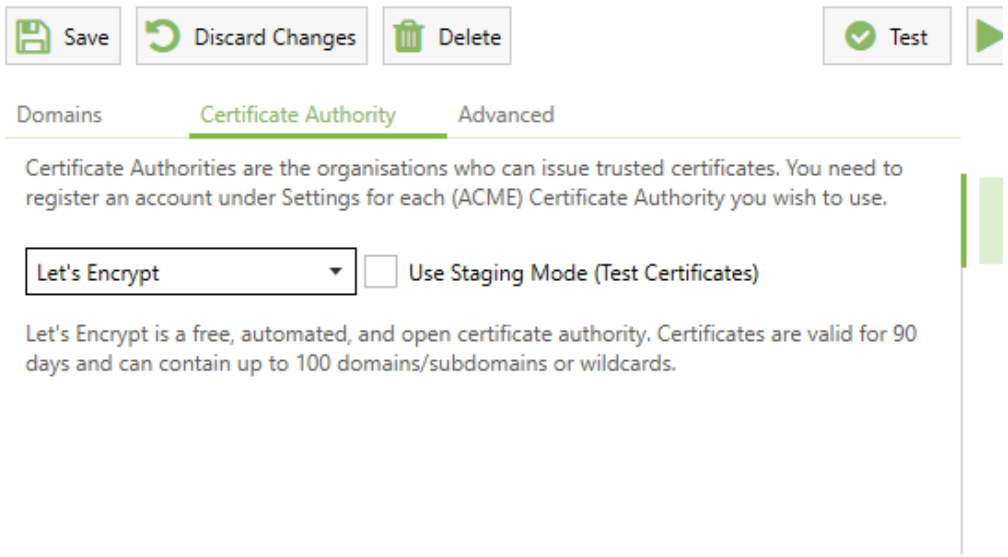
Each certificate may cover multiple domains. You can easily add or remove domains from a certificate and auto-populate the list of domains from existing website bindings (e.g. IIS).

Depending on the Certificate Authority you choose, your certificate can include a **single domain, multiple domains (SAN (Subject Alternative Name)) or domain wildcards** (e.g. *.certifytheweb.com) to cover multiple sites or services.

Your Choice of Certificate Authorities

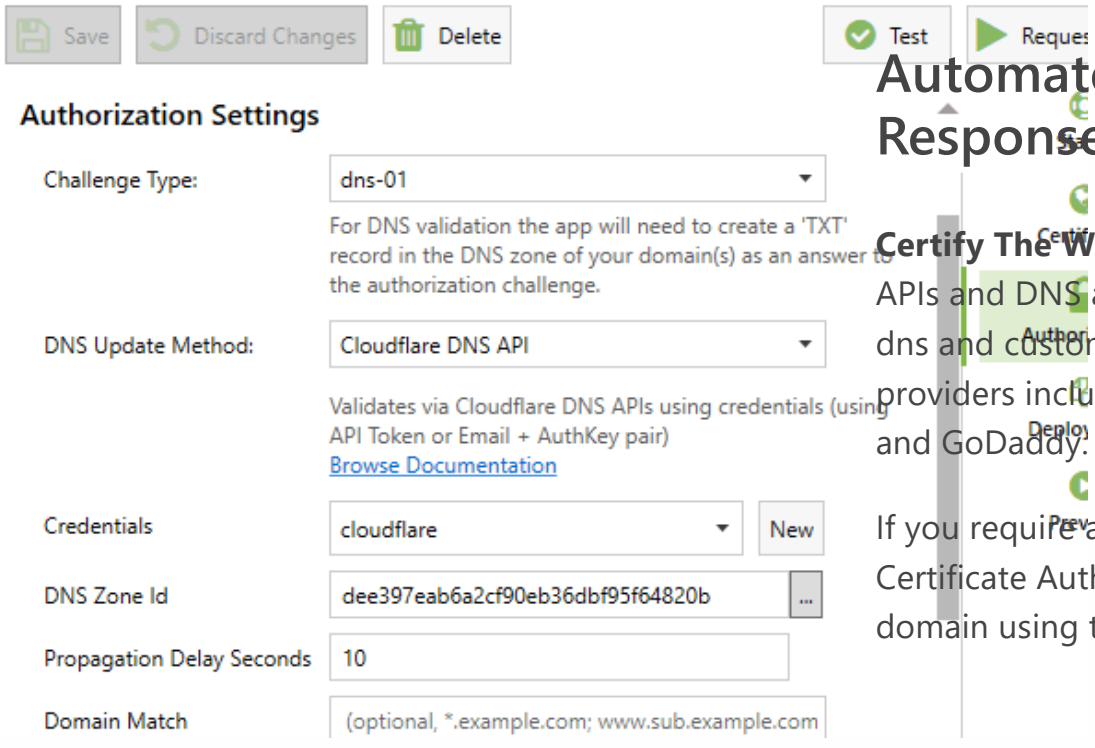
The current most common automated Certificate Authority is **Let's Encrypt**, a free Certificate Authority (letsencrypt.org). You can also choose from other **ACME** (Automated Certificate Management Environment) Certificate Authorities, such as **BuyPass Go SSL**, **DigiCert** or a custom certificate authority (such as smallstep or Keyon true-Xtender Enterprise PKI).

If required, each Managed Certificate can use a different Certificate Authority and you can mix use of Production or Staging (Test) certificates.



Multiple Ways To Validate Your Domain

Certificate Authorities will require you to prove you control the domain you are requesting a certificate for (Domain Validation). The most common method is an automated **Challenge Response** via http (presenting a specific file at a url on your domain) or DNS (add a specific TXT record to your domains DNS). This complex process is handled for you automatically by the software.



Automated DNS Challenge Response

Certify The Web has support for over 36 different DNS APIs and DNS automation methods (including acme-dns and custom scripting options). Popular DNS providers include Cloudflare, AWS Route53, Azure DNS and GoDaddy.

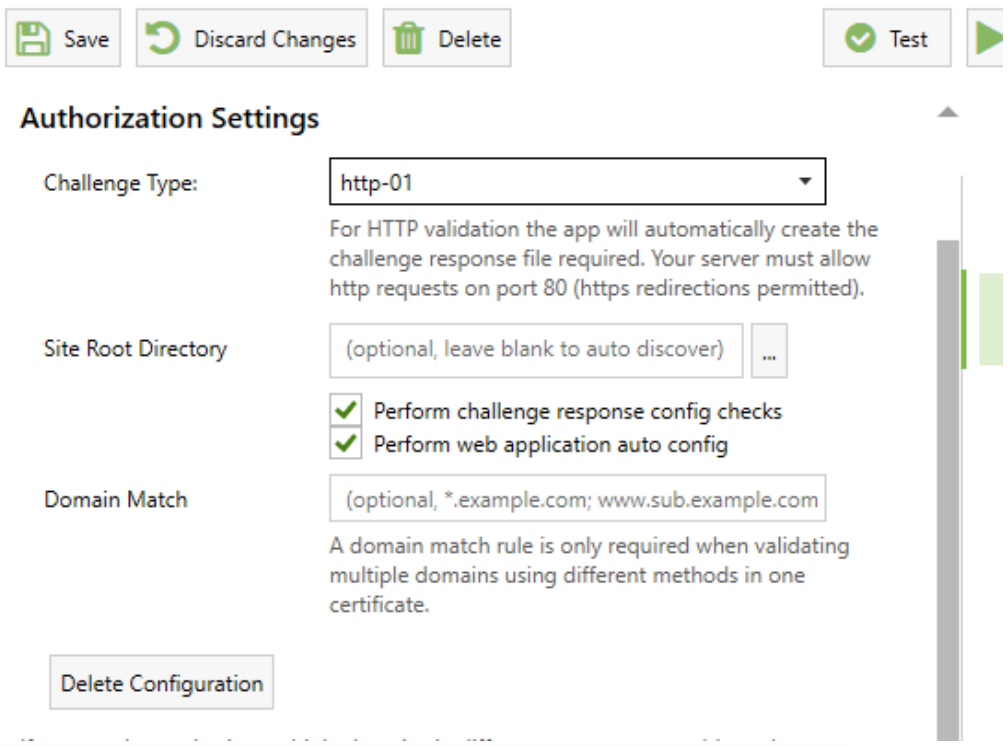
If you require a wildcard certificate for a domain, most Certificate Authorities require that you validate your domain using the DNS method.

Automated HTTP Challenge Response

Our built-in dynamic http challenge server means you can automatically serve http challenge responses to the Certificate Authority (via port 80) without requiring http bindings on your website and without interrupting normal traffic to your website.

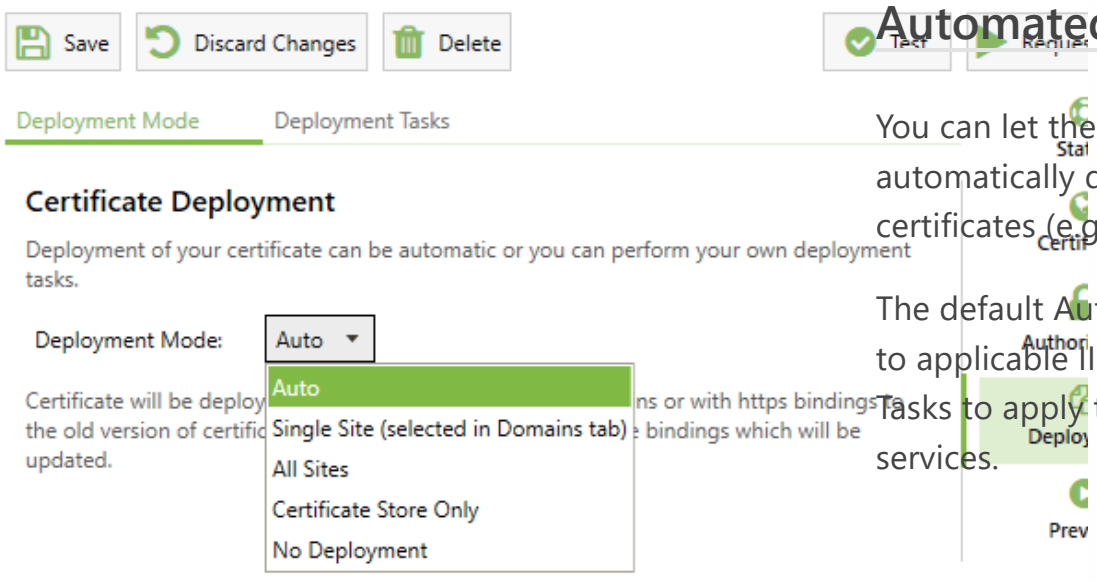
When port 80 is in use by a non-http.sys based service (such as Apache httpd) you can fallback to serving challenge responses via your web server.

Domain validation methods can be mixed as required within a single certificate order depending on your requirements.



Powerful Deployment Options

Whether you need simple auto deployment to IIS or advanced deployment to other services/servers or remote certificate stores, **Certify The Web** has extremely powerful options for sophisticated deployment.



Automated Deployment

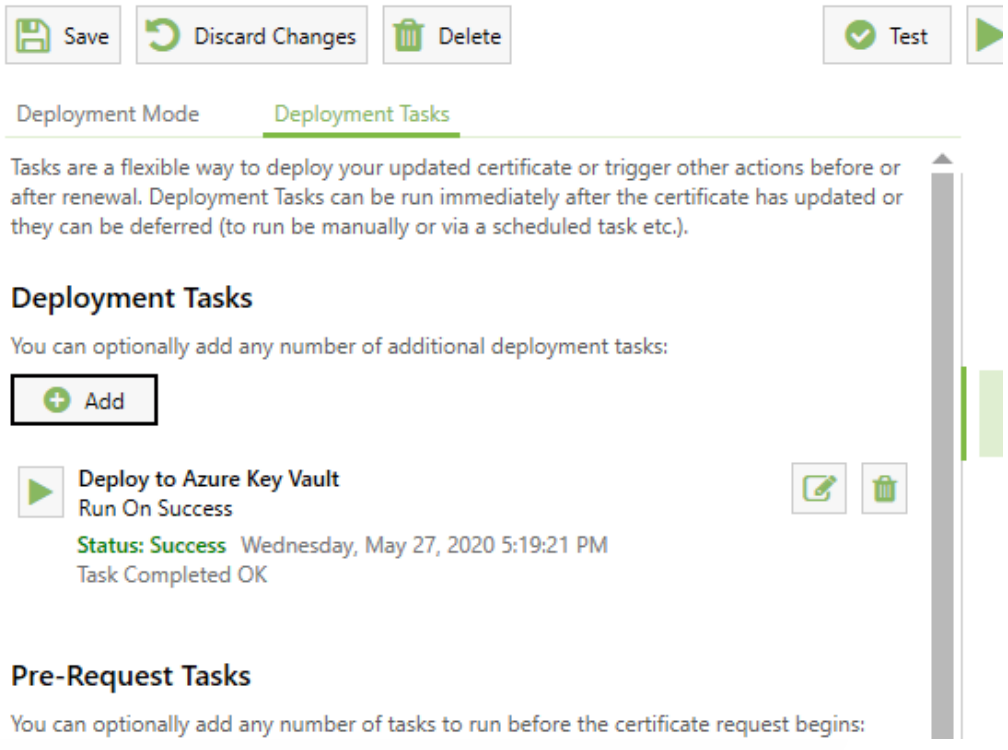
You can let the app auto-renew certificates then automatically deploy them to the services that use the certificates (e.g. IIS websites).

The default Auto Deployment will apply your certificate to applicable IIS websites, or you can use Deployment Tasks to apply the latest certificate to a range of other services.

Deployment Tasks

Deployment Tasks are a powerful way to make use of the certificates you manage through the app. You can deploy and use your certificate in an unlimited number of ways, including:

- MS Exchange, Remote Desktop Services
- Microsoft Azure Key Vault
- Central Certificate Store (CCS) via local or UNC paths
- Apache, nginx, Tomcat and other services using PEM/CRT/chain certificate files
- SFTP and SSH support
- Scripting (such as a PowerShell or linux shell scripts)

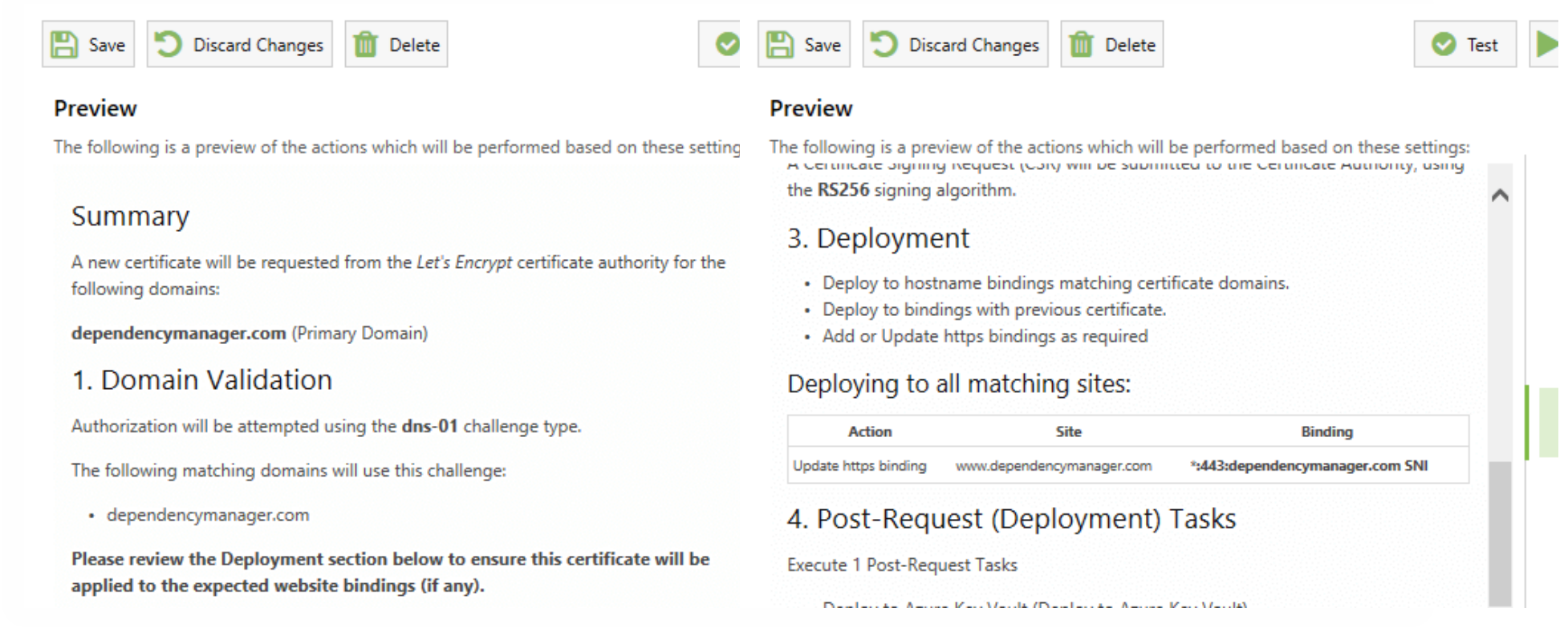


Previewing Renewals

The Preview tab shows the planned actions to be carried out during the next certificate request or automatic renewal, including:

- Domains to be included in the cert
- How domain validation will occur

- The automated website bindings (IIS) which will be applied/updated (if applicable).
- Deployment Tasks such as installing your certificate on MS Exchange, exporting to Apache, nginx, Central Certificate Store (CCS), SSH/SFTP exports etc

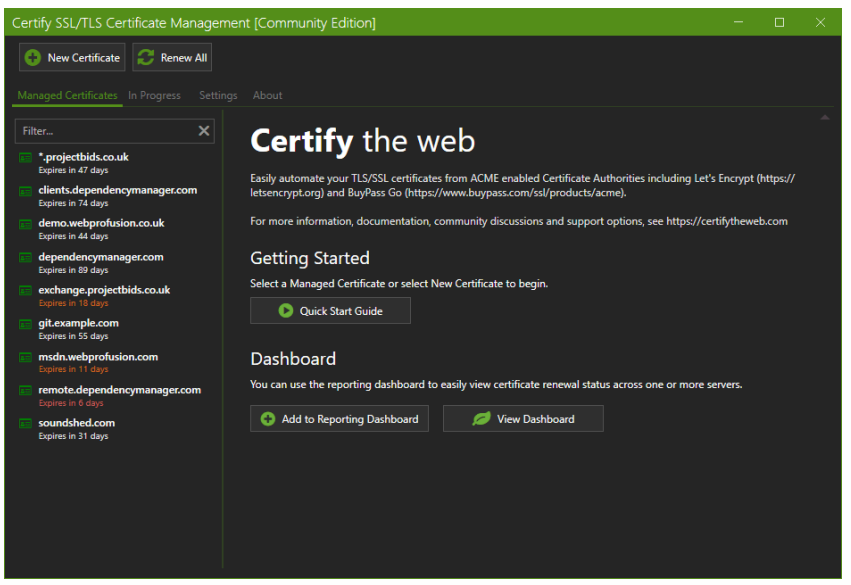


Plus Much More..

The software is constantly being improved and refined, so be sure to stay up to date with the latest version. There are many other features and details to be explored, so check out the documentation.

Dark Mode

And last but not least, there's **Dark Mode**. The easy on the eye, and arguably much cooler, alternative to Light mode.



Get Started

To get started using **Certify The Web**, download the latest version and try it out.

System Requirements

- The software will normally run on the server which is running your website or service, especially when http domain validation is required.
- Windows Server 2012 R2 64-bit or higher (Windows 10 included), .Net 4.6.2 or higher installed.
- Certificates from the Let's Encrypt Certificate Authority expire every 90 days, so you must use the default Auto Renew feature or request a new certificate manually.
- This software depends on services from trusted Certificate Authorities such as Let's Encrypt. Service interruptions associated with certificate authorties are outwith the control of this application.

Privacy Policy