TECHNICAL BRIEF

Gain full visibility of TLS certificates with Venafi TLS Protect Cloud

Powerful discovery services give you a complete inventory of public- and private-facing TLS certificates

Venafi TLS Protect Cloud Technical Brief

Purpose: This technical brief describes the services provided by Venafi TLS Protect Cloud to discover and add public- and private-facing TLS certificates to a central inventory.

Why this information is important: Outages caused by expired TLS certificates lead to expensive downtime and ongoing customer and employee dissatisfaction. Discovery services give you a complete view of certificates in your environment and their expiration dates.

What TLS Protect Cloud adds:

- Discovers public facing certificates and those on private networks
- Starts building an inventory as soon as you start using it
- Runs on-demand or on a schedule
- Enabled through the console or programmatically

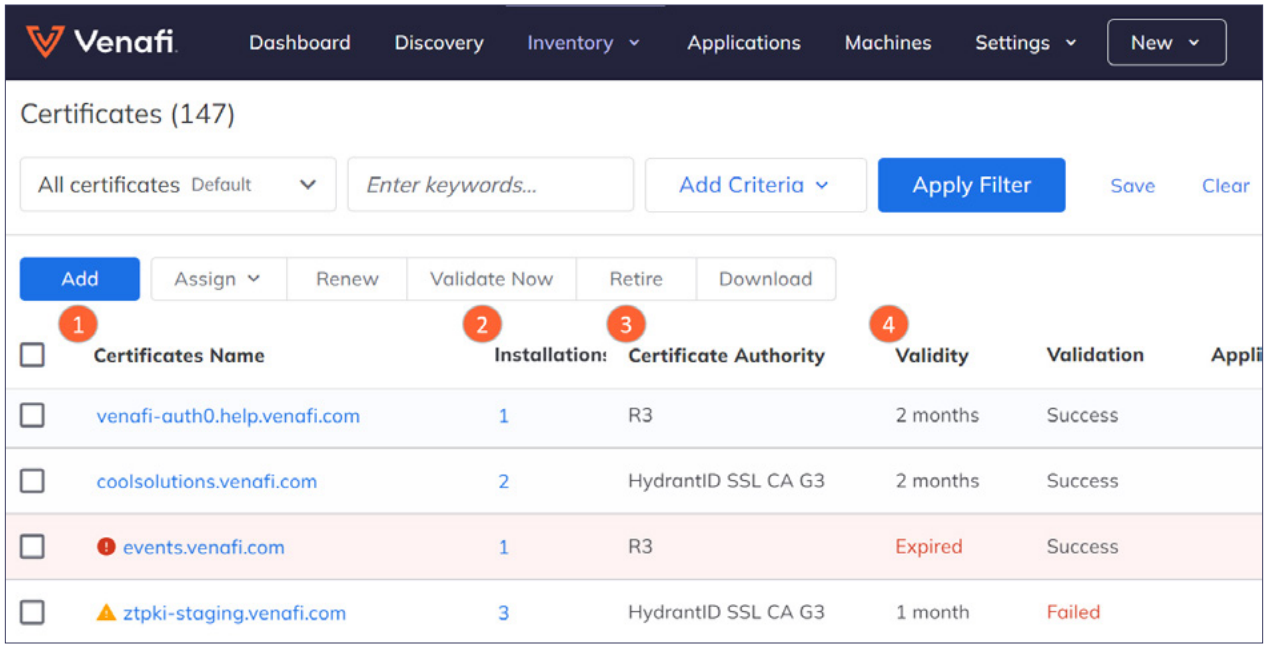
With the growing number of TLS machine identities, or TLS certificates, that are prevalent in organizations today, the only way to build and maintain an accurate inventory is with automated discovery services. And without an accurate inventory, you're blind to certificates nearing expiration, certificates with potential vulnerabilities, or those that do not comply with established security policy. This document briefly describes the discovery services available in Venafi TLS Protect Cloud.

Internet Discovery for Public Facing Certificates

Typically, the first discovery you'll run with TLS Protect Cloud is an internet discovery. This service will discover internet-facing certificates that are outside of your organization's private network. Internal discoveries are created by default and will run automatically when you sign up for a free 30-day trial. Upon registration, they extract the domain from the email ID you register with and begin searching for public facing certificates on that domain. Of course, you can change the default settings later and easily enter other domains to search.

Internet discovery immediately provides useful information. For example:

1. Certificates and certificate metadata such as CN, SAN, Chains and expiration dates.
2. Number of times a certificate is installed and the IP addresses and ports where it's being used.
3. Which CAs issued your certificates, useful for identifying any certificates issued from unapproved CAs.
4. How much time remains in the validity period, useful for flagging certificates that may expire soon or are coming up for renewal.



You'll also automatically get information about certificate installations. For example:

5. Validation status to determine if there are any configuration errors which may cause disruptions to service, such as incomplete chains or certificates that fail to align with DNS information.
6. Chain validation, so you can easily flag things like incomplete chains or self-signed certificates that may not fit within your organization's policy.
7. Insecure configurations of TLS protocols to help you mitigate potential audit findings.

Discover Private (Internal) Certificates

For certificate discovery inside your company's network, TLS Protect Cloud provides both a basic and enhanced discovery service so you can quickly find and monitor privately issued TLS certificates, even across distributed and segmented networks.

The Basic service lets you manually run a quick certificate discovery inside your organization's network by targeting a TLS port or port range or by targeting FQDNs, IP addresses or CIDR blocks. The Enhanced service also discovers certificates inside your network and offers additional capabilities like scheduling and automatic validation for discovered certificates. Certificate validations help ensure that you're installing and using your certificates in a way that best secures your machine identities.

Start today with TLS Protect Cloud

By starting with a comprehensive discovery of TLS certificates, you are well on your way to taming the chaos and managing these machine identities to prevent outages and security breaches. Try it for yourself. Sign up now for a free 30-day trial of TLS Protect Cloud to discover what's on your network https://venafi.com/try-venafi/tls-protect/