Venafi

TECH BRIEF

Venafi TLS Protect Cloud Ensures New Certificates Meet Security Policies

TLS Protect Cloud makes issuing policy-compliant TLS certificates easy, error free and highly scalable

Technical Brief

Purpose:

This technical brief describes how Venafi TLS Protect Cloud makes it easier for machine identity owners to issue TLS certificates.

Why This Information Is Important:

TLS certificates are a critical security asset for both authentication and protecting data in transit. It's critical to have policy that clearly states how they should be created and managed, as well as providing owners with an easy way to issue certificates that meet policy criteria.

What TLS Protect Cloud Adds:

- Lock down security policies for new certificates by creating issuing templates
- Create unique templates to support different teams and use cases
- Facilitate self-service where owners can directly request policy-compliant certificates
- Reduce errors by pre-populating and locking certificate attributes

When it comes to setting policies for how TLS certificates should be created, NIST[i] provides excellent, detailed guidelines. The guidelines touch on identifying approved Certificate Authorities (CAs), certificate validity periods, certificate details such as signing algorithm, key length and subject DN and SAN contents and much more.

Even with a written policy, it can be challenging for resource owners to follow when they request TLS certificates for the systems and applications they are responsible for. They may not be familiar with the security policy or use it that often. The purpose of this document is to outline capabilities in Venafi TLS Protect Cloud that make it easy for resource owners to quickly and securely issue TLS certificates that comply with organization security policy through the use of issuing templates.

An issuing template can prove beneficial to both InfoSec and resource owners. InfoSec can set up issuing templates with rules in place that meet their organization's security policy. Resource owners can then use issuing templates as a quick and error-free way to securely issue certificates for their systems and applications.

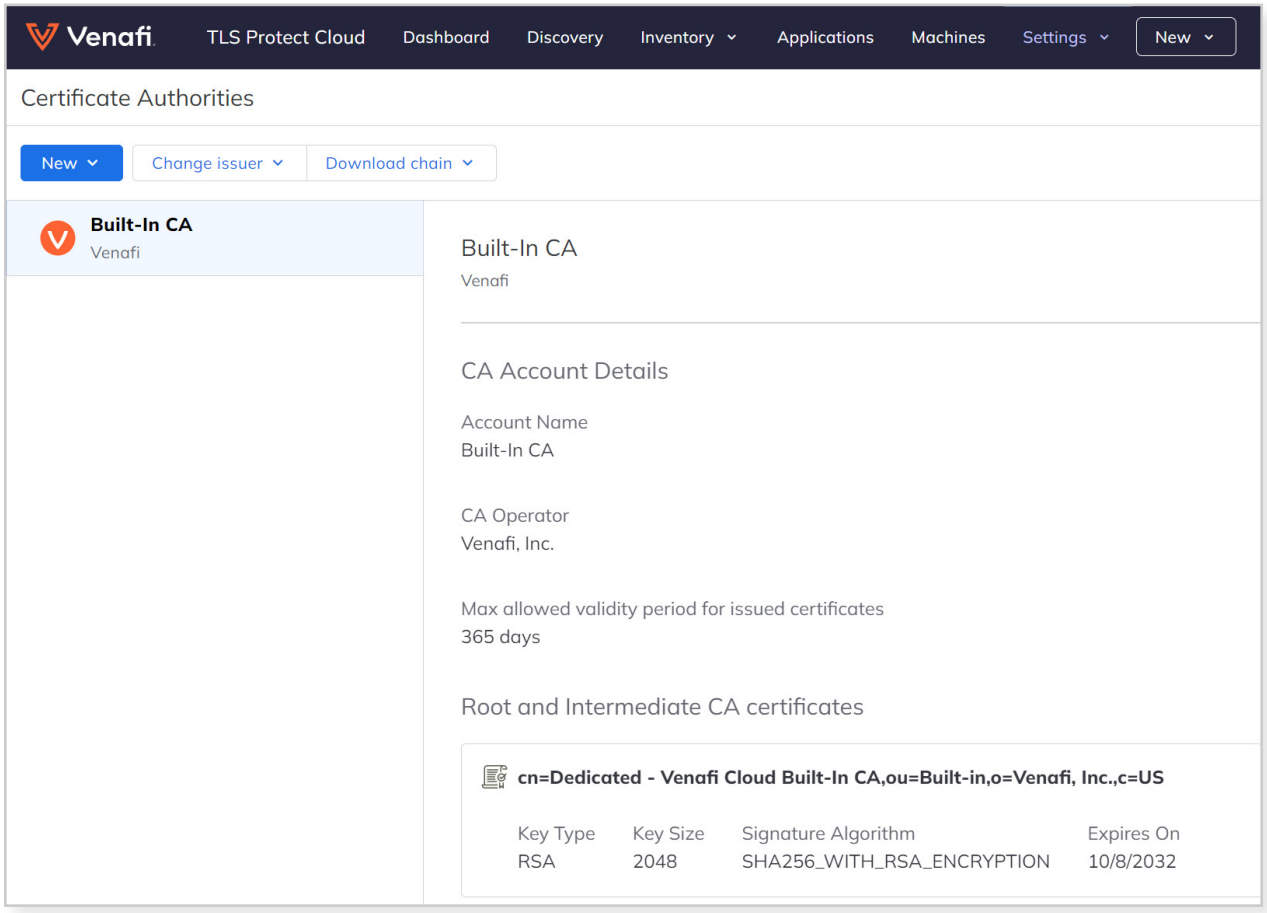
i NIST SP 1800-16: Securing Web Transactions, TLS Server Certificate Management
https://csrc.nist.gov/publications/detail/sp/1800-16/final

Identify the Certificate Authority (CA) to Issue a Certificate

The first step in setting up an issuance template is to identify which CA the certificates will be issued from that template. Most organizations work with multiple Certificate Authorities for public-facing certificates and will use one or more CAs for private certificates for internal networks. In fact, using multiple CAs is recommended to allow for a quick switch between providers in case a CA is compromised in any way.

Different CAs may be used for different use cases. For example, an organization might choose to enable owners of public-facing certificates to issue certificates from a high-profile CA such as DigiCert or Entrust, while owners of private-facing certificates will use Microsoft AD CS or the built-in CA provided by TLS Protect Cloud.

In the example below, the built-in CA from TLS Protect Cloud is configured as the Certificate Authority for an issuing template.



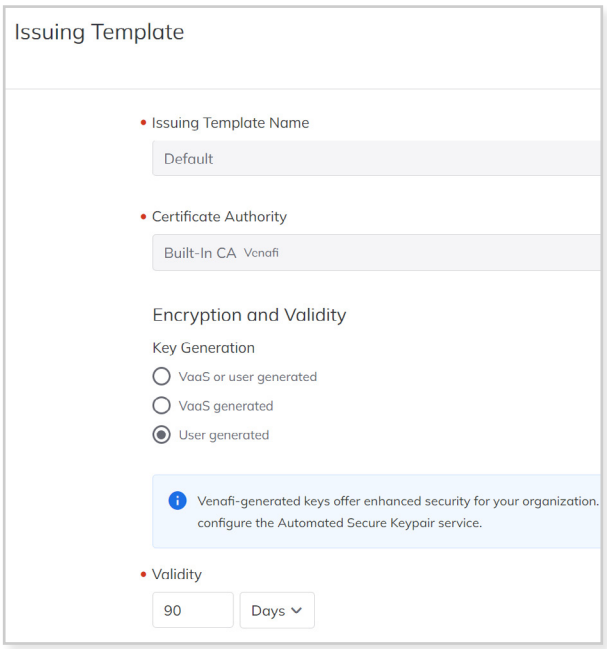
Set the Rules for Certificates Issued Using the Template

Once the Certificate Authority is configured, the next step is to set the rules for certificates issued through the template. There are multiple settings, and while many are optional, it's recommended to provide and lock as many settings as possible. Locking fields makes it easier for resource owners, as they have fewer fields to complete. This policy can increase speed and reduce the potential for errors when having to complete fields on their own.

Issuing template fields that benefit from preconfigured policies include:

- The default Validity Period (Recommended value is 90 days. Minimum setting is 1 hour)
- Common Name, Subject Alternative Names, and CSR Parameters fields
- Key Algorithm Type
- More

Once the issuing templates are created, the final step is for resource owners to add them to their applications, and then submit certificate requests using the issuing templates. For example, if I'm a network administrator responsible for F5 load balancers, I can assign an issuing template to my F5s applications in TLS Protect Cloud so whenever a certificate is requested, it follows the settings in the template. Once submitted, the request is automatically sent to the specified CA, and in an instant, the new TLS certificate will be ready to install either manually or automatically via TLS Protect Cloud push- or pull-provisioning.



See how easy it is to issue policy-compliant TLS certificates

By leveraging issuing templates in TLS Protect Cloud, security teams can give certificate owners the ability to quickly and easily get certificates needed for their systems and applications that meet the organization's security policies. Sign up now for a free 30-day trial of TLS Protect Cloud and test out our issuance templates for yourself **https://venafi.com/try-venafi/tls-protect/**

Venafi is the cybersecurity market leader in machine identity management, securing the cryptographic keys and digital certificates on which every business and government depends to deliver safe machine-to-machine communication. Organizations use Venafi key and certificate security to protect communications, commerce, critical systems and data, and mobile and user access. **To learn more, visit venafi.com**