This white paper provides information about installation, usage, and Outcomes of TLS Certificate Management App for ITOM Visibility customers.
# Table of contents

**Introduction** 3

- How it works 3
- App Installation and Discover Setup 4
- TLS Certificate Management App—Outcomes 5

**Conclusion** 9

**For more information** 9
Introduction

Compliance and security hygiene go hand in hand. Lack of visibility to deployed TLS certificates and expiry of TLS certificates result in service outages and data breaches. The latest data breach from the largest consumer credit reporting company said “TLS certificate had expired about 10 months before the breach occurred, meaning that encrypted traffic was not being inspected throughout that period.”

The ServiceNow® Certificate Inventory and Management solution provides a platform-based approach to the lifecycle management of TLS certificates. This solution combined with task fulfilment can provide a methodical approach to request management and renewal management. Automating manual tasks such as requests for new certificates and the renewal of expired certificates increases the productivity of the public key infrastructure (PKI) team by ~30% and helps to digitize their manual workflows.

The ServiceNow® Certificate Inventory and Management solution allows you to discover and take inventory of all your deployed TLS certificates, keeps you informed of impending expirations, creates certificate tasks via flows to renew expiring certificates, creates incidents for already expired certificates, and prioritizes certificate importance. This feature helps you proactively manage your certificates, avoid manual tracking of a large volume of certificates, and will prevent costly outages due to expired or expiring certificates.

How it works

Certificate Inventory and Management allows Discovery capability from ServiceNow ITOM to automatically scan for certificates on specific ports through your existing discovery schedules. The solution also provides comprehensive ways to scan application URLs to auto discover the TLS certificates in to ServiceNow CMDB.

Figure 1: Architecture Diagram of TLS Certificate Management app

“ The ServiceNow® Certificate Inventory and Management solution provides a platform-based approach to the lifecycle management of TLS certificates. This solution combined with task fulfilment can provide a methodical approach to request management and renewal management.
Port scan Discovery: As part of the Configuration Management (CI) Discovery process during Shazzam, the MID Server executes scanners to collect the certificate chain information from the IP port number defined in the out of box tables. The discovery scan captures various certificate attributes and other data including certificate hierarchy.

The MID Server transforms the certificates to an XML payload containing the certificate information and shares the XML payload with the instance. The Shazzam sensor on the instance picks up the ECC queue entry and adds a new record into the Discovered Certificate cmdb_ci_certificate table. The port probe tls_ssl_certs automatically scan 14 default preauthorized ports some of which are 443, 8443, 9443, 636 (ldaps), 993 (imaps), 995 (popssl).

URL Discovery: The Certificate URL sn_disco_certmgmt_cert_url table holds a list of URLs to target for certificate discovery. Each record also has an optional reference to the Unique Certificate cmdb_ci_certificate table, to see what certificate is related to the given URL definition.

App Installation and Discovery Setup
The app is available via the ServiceNow Store for ITOM Visibility customers. In order to use the app ServiceNow instance must be upgraded to Orlando and the Visibility com.snc.itom.visibility.license and the Discovery com.snc.discovery plugins should be installed and activated. After that you can download the Certificate Inventory and Management application from the ServiceNow Store.

Discover certificates via Ports scan
1. Activate the TLS port probe tls_ssl_certs, Navigate to Discovery Definition > Port Probes. Open tls_ssl_certs. Click the Active checkbox to enable the probe and then save your changes. This box will be unchecked by default for any new installation.
2. Add IP service to help configure the TLS port probe by navigating to Discovery Definition > IP services. You can create a new IP service with a port.
3. Configure the TLS port probe. You can add additional ports, or remove any existing ports, by editing the Port Probe definition. Navigate to Discovery Definition > Port Probes, open tls_ssl_certs, click on the lock icon next to Triggered by services to unlock this field. Delete or add more ports from the search area and then save your changes.

"The ServiceNow® Certificate Inventory and Management solution allows you to discover and take inventory of all your deployed TLS certificates, keeps you informed of impending expirations, creates certificate tasks via flows to renew expiring certificates, creates incidents for already expired certificates, and prioritizes certificate importance."
Discover certificates via URL

1. Navigate to Certificate Management > Certificate Discovery Source URLs, click New to add individual URLs to the table.

2. Make sure to enter URLs in this format to ensure accurate results. The port is optional and defaults are used if the port is not provided: scheme://host:port, e.g., https://www.servicenow.com or https://servicenow.com:443.

3. Create a Discovery schedule, chose Certificates from dropdown named Discover, Select Certificate Discovery Type: URL Certificate Discovery. Leave the batch size as it is, unless recommended to change.

4. From the Certificate URLs tab, click Edit to add or delete other URLs and then click Submit.

Existing and new Discovery schedules for URL discovery should then automatically scan for any certificates on the specified ports and URLs and populate the certificate details into sn_disco_certmgmt_certificate_history table.

TLS Certificate Management App—Outcomes
Centralized repository and metadata extraction for all certificates:

Certificate Inventory and Management allows Discovery capability from ServiceNow ITOM to automatically scan for certificates on specific ports through your existing discovery schedules.
**Unique Certificate**

**V-ubuntu-Jboss (Certificate Management View)**

**Subject common name**: V-ubuntu-Jboss

**Issuer**: V-ubuntu-Jboss

**State**: Installed

**Valid from**: 2017-12-07 00:00:00

**Valid to**: 2018-12-07 00:00:00

**Serial number**: 00 c8 14 de e2 fd 4a 56 b4

**Description**

**Additional certificate details**

**Subject alternative name**

---

**Diagram**

[Diagram of network connections and certificate management view]
Out-of-the-box workflows for creating and assigning Tasks for To-be-expiring and already-expired certificates:

Dashboard Insights to track to-be-expiring and expired certificates:
Flow designer capability can automatically create alerts or incidents to track the expiry of TLS certificates:
Conclusion

TLS Certificate Management application empowers your organization to manage your entire set of Public Key Infrastructure (PKI) operations—visibility of all certificates, task workflows and expiration pipeline. It will also be a huge benefit in terms of preventing the service outages and the associated revenue and security loses caused due to expired certificates.

For more information
www.servicenow.com