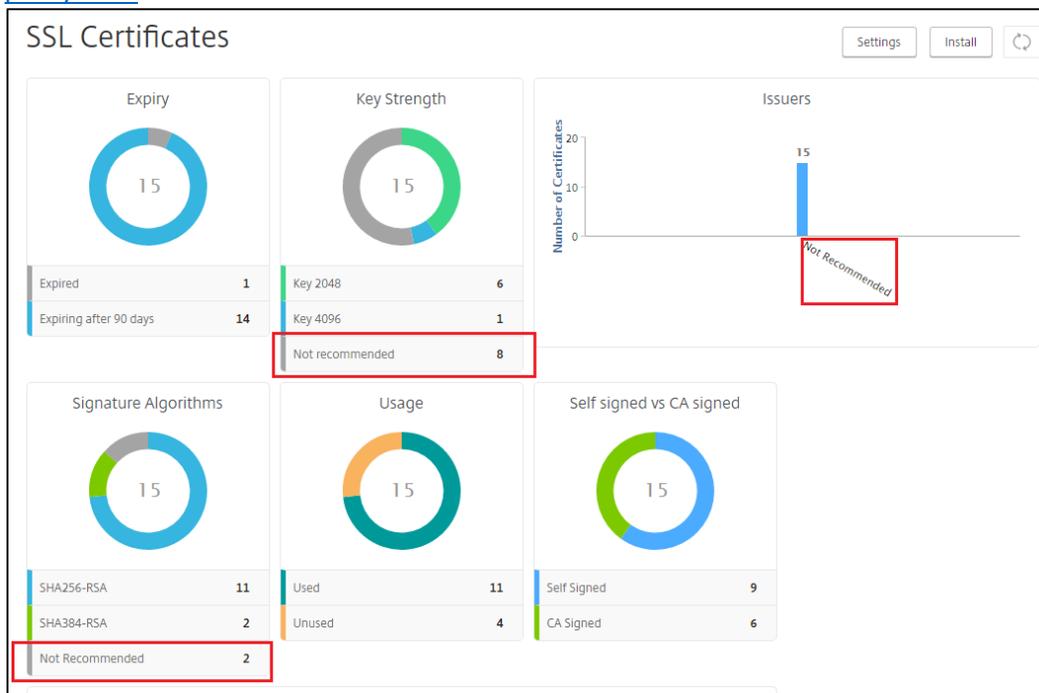**How do I perform complete SSL Certificate monitoring and management using NetScaler MAS**

NetScaler Management and Analytics System allows you to perform complete SSL Certificate monitoring and management operations from one single console.

When a NetScaler appliance is discovered in MAS, all the certificates that reside on the NetScaler appliance also get copied to MAS. This gives MAS the visibility into all the certificates across all of the managed NetScaler devices thus becoming the perfect solution for complete SSL Certificate management and monitoring. Let us take a look at some of the use cases that MAS helps with:

- Every Enterprise has its own SSL Policy wherein the enterprise defines the minimum requirements that all SSL Certificates must adhere to. For example, Enterprise ABC mandates that all certificates must have minimum key strengths of 2048 bits and must be authorized by trusted CA/issuers. Any non-compliance with this policy, is required to be highlighted and bought to the notice of the administrators.
  MAS now helps with such scenarios wherein an admin can configure Enterprise SSL Policy settings and MAS clearly highlights any non-compliance with the 'Not Recommended' tag.
  To know more configuration details, please see this link -> http://docs.citrix.com/en-us/netscaler-mas/11-1/certificate-management-how-to-articles/how-to-configure-enterprise-policy.html

- Administrators need to regularly monitor the expiry dates of SSL certificates' to ensure that certificates get updated before they expire. Getting proactive alerts via email/sms 'x' days before a certificate's expiry is as much valuable as seeing the status of a certificate's expiry on the dashboard. Such timely notifications/dashboard charts help administrators take the necessary corrective steps well in advance. MAS helps send proactive alerts to administrators on the expiry status of their certificate as well as captures the expiry details on the SSL dashboard. To know more configuration details, please see this link -> http://docs.citrix.com/en-

- Administrators no longer need to login to individual NetScaler devices to upload certificates, update certificates, create CSRs, link/unlink SSL certificates, etc. All these popular SSL certificate management operations can be performed from MAS itself thereby improving an
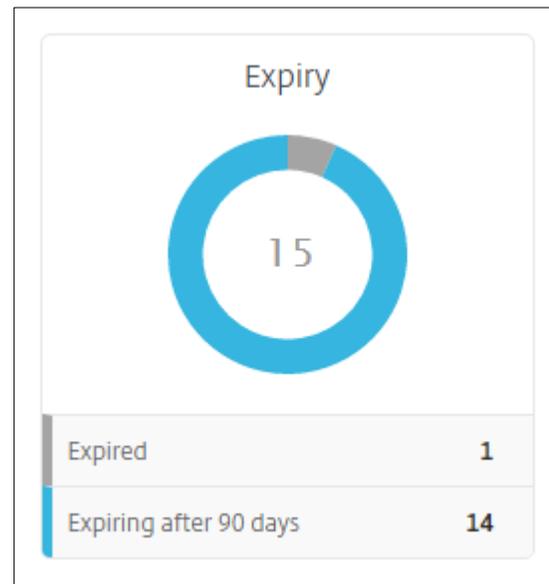

administrator's efficiency.

For configuration details, please refer to the following links ->
  - http://docs.citrix.com/en-us/netscaler-mas/11-1/certificate-management-how-to-articles/how-to-install-ssl-certificates-on-netscaler-instance.html
  - http://docs.citrix.com/en-us/netscaler-mas/11-1/certificate-management-how-to-articles/how-to-update-an-installed-certificate.html
  - http://docs.citrix.com/en-us/netscaler-mas/11-1/certificate-management-how-to-articles/how-to-link-and-unlink-ssl-certificates.html
  - http://docs.citrix.com/en-us/netscaler-mas/11-1/certificate-management-how-to-articles/how-to-create-csr.html

- Lastly, the dashboard itself helps administrators with multiple use cases. For example an administrator may have uploaded a certificate but may have forgotten to put it to use by binding it with a virtual server. The SSL dashboard clearly highlights to the administrator any such certificates that are installed but are still unused.
The dashboard being completely clickable, allows administrators to directly click on the required problem area and drill down for more details on the certificates.
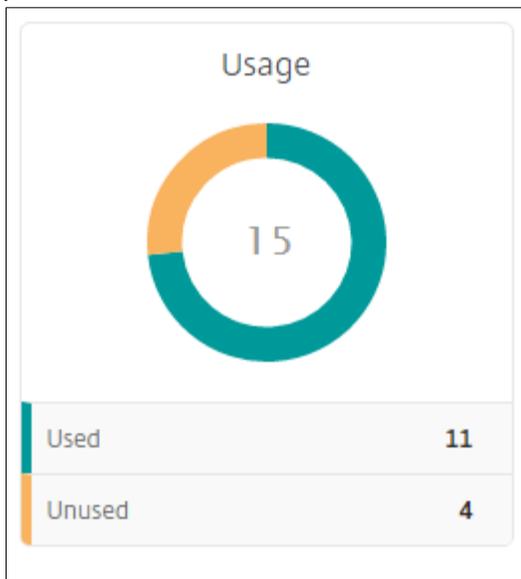
To explore the plethora of SSL certificate management features that MAS offers, you may download the NetScaler MAS for free at https://www.citrix.com/downloads/netscaler-mas.html