Why Web-Based Authentication?

Why Web-Based Authentication?

- To authenticate guest users

  It is essential for organizations to provide network access to temporary users such as guests and contractors. Guest users are most likely to use devices that are beyond the control of an organization's IT services. As a result, temporary users are not going to have endpoints configured for IEEE 802.1X. Web authentication is a convenient mechanism to have such users authenticate and sign an acceptable user policy. Authenticating temporary access users also has the added benefit of making it possible to monitor their activities, allowing organizations to meet compliance requirements.

- As a fall back authentication mechanism for regular network users

  Often, regular network users with devices configured for IEEE 802.1X devices are likely to fail authentication. This can happen for various reasons like expiration of passwords or certificates and misconfigured supplicants. Web authentication provides a means for such users to authenticate themselves and remediate issues that are preventing them from authenticating through IEEE 802.1X.

- Device registration

  Users often have personal devices, like tablets and smartphones, that they use to access the Internet and other corporate applications. It is increasingly important for IT to be able to link every such device to a user to help ensure that it has appropriate access to network resources. Web authentication can be used as a means to allow users to register their personal devices. Once registered, the device can be either given full or limited access to network resources based on the organization's security policy and the user's role in the organization.