Single Sign On FAQ

What is Single Sign On?

Single Sign On (SSO) requires just one login to access EMC applications and portals, rather than entering your password for each EMC application. We already deployed SSO for a number of portals and applications such as Employee Central, InfinIT, and Salesforce.com. The new browser login page reflects our newly expanded SSO capabilities, providing easier access for you while maintaining the same level of security on the network.

I login when turning on my computer, isn’t that enough?

Your initial Windows/Network login grants you access to your computer. However, SSO enables you to access EMC-related applications or websites by inputting your Windows/Network credentials once per browsing session. Also, as EMC is no longer a single-browser, single-device company, the SSO login page enables a more consistent experience when accessing the applications and sites you need for your job.

When will I have to login?

A login will be required upon your first visit to a SSO-enabled EMC application or portal during each new browser session. For example, if you login and then close your browser or reboot your computer, you will need to re-enter your EMC username and password when you return to an EMC SSO protected resource.

Is a login required when visiting a non-EMC site?

No. If you open your browser to visit a non-EMC site, you will not be required to enter your EMC credentials. A login is only required upon your first visit to an EMC-secured application or site.

Why do I have to repeat a login each time I open a new browser?

This is a standard security measure that existed prior to the new SSO login page. Each authentication is unique to one browser session to protect EMC resources.

Can I just leave my browser open to avoid having to re-enter my username and password?

Your SSO login will remain valid for a period of 24 hours as long as you do not close the browser session and have been accessing the application every 2 hours. If the SSO login expires, then you will have to re-enter your login. This timeframe may be different depending on the application requirements, and could change in the future as we continue to enable the strongest user experience while keeping within our best security practices.
Will I need an RSA FOB/Token on the SSO login page?

You will be prompted to use the RSA FOB/Token only when accessing privileged applications that require it. The SSO login page will make it very clear whether you are being prompted for only your Network/Windows login information, or for your RSA FOB/Token.

Your RSA/FOB Token is still required for all remote EMC network access through VPN.

As a Mac user, I’ve often had to use my VDI to access a number of portals. Will SSO remedy that?

No. Although the SSO login page will provide all EMC users with a consistent login screen, it does not change the need to use VDI to access certain applications.

Will more EMC applications and portals become SSO-enabled in the future?

Yes. We are continuing to expand the list of SSO-enabled sites, including Concur, UBS, and additional mobile assets and applications, improvements to RSA token management, the PasswordPortal and more.