Kerberos password synchronization with Active Directory

Why it's important

Over the last few years, more and more third-party applications and services commonly used on MIT campus integrate with MIT's Active Directory (AD) service for authentication, rather than talking directly to our Kerberos service. Recent examples include Microsoft Exchange email and calendaring, MIT's secure wireless network, and others. For this reason it has become more and more important to keep Active Directory synchronized with Kerberos, to provide a consistent experience across services and allow all members of the MIT community to use applications and services seamlessly regardless of which authentication technology they rely on behind the scenes.

How it works

Background

MIT runs two central Active Directory (AD) services as well as our Kerberos authentication service. One Active Directory service is associated with the EXCHANGE.MIT.EDU domain and the other with the WIN.MIT.EDU domain. Synchronizing passwords (i.e. setting a user's password in Active Directory to be the same as her Kerberos password) has been happening automatically since 2008 for the EXCHANGE.MIT.EDU Active Directory service, and since 2010 for the WIN.MIT.EDU Active Directory service. This has been working quite well, and for any member of the MIT community who has changed their password since those dates, the password has been seamlessly synchronized with Active Directory. However, it has not included members of the community who have not changed their passwords since those dates.

What's new: Password sync at certificate renewal

Beginning with MIT personal certificate renewal in the summer of 2012, the MIT Certificate Server (ca.mit.edu) will also automatically synchronize passwords with Active Directory at the time you renew your certificate. Unlike the older synchronization methods, this does not require you to change your password. It will simply set your Active Directory passwords to be the same as your current Kerberos password behind the scenes, if they have not been synchronized before.

The process for getting a new certificate will look and feel the same. You should not notice any difference. However, after you do so you will be able to use applications and services relying on Active Directory for authentication seamlessly using your current Kerberos password.

Caveats

- Members of the MIT community are still strongly encouraged to change their Kerberos password regularly. It is recommended that you change your password about once a year. Along with picking secure and difficult to guess passwords, changing your password regularly can be a helpful tool in keeping your account secure and preventing it from being compromised.
- Maintaining different passwords between the MIT Kerberos service and Active Directory is not supported. If this presents a problem for you, please contact us at helpdesk@mit.edu or 617-253-1101 so we can explore work arounds for your specific use case.