THOMAS STEWART

Cloud Identity Summit
July 21, 2010

Why are we here?

Cloud **Identity** Summit

Why are we here?

How do we make it work?

How do we make it work efficiently, with our current infrastructure?

With our existing user identities?

…and not give up too much


Thereifixedit.com

Early Adopters

Synchronize ID's and Passwords

Standards Help

OpenID

SAML

WS*


Thereifixedit.com

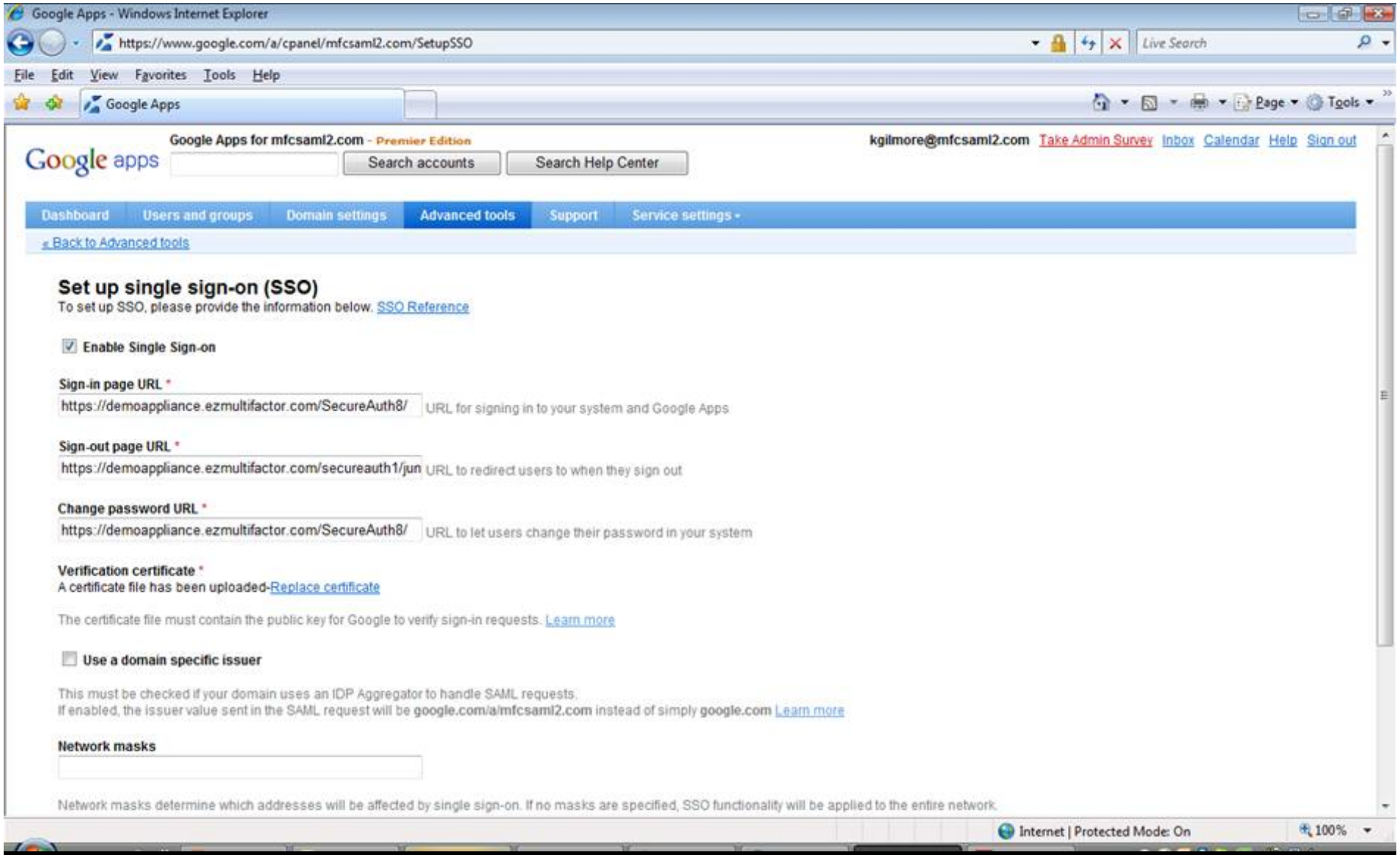
How would Google do it?

Not like this

…or this

How would Google do it?

target redirect to IdP



Google lets the enterprise take control of the authentication

Central Authentication

- The concept of target-redirect, separate service for authentication is not new
  - Access managers like SiteMinder, Oblix TAMeb
  - Application servers like WebSphere, .NET
- Doing authentication on the application is restrictive
  - Limits yourself to vendors supported authentication
  - And you have to TRUST their methods

Done right

SecureAuth®

Identity Enforcement Platform

IEP – all in one solution

Combining your existing directory if IDs:

- Authentication
- Single Sign On
- Simple User Management

IEP – all in one solution

- Secures and simplifies your evolving environment:
  - Applications
    - Multi-tenant public cloud, “private” cloud
    - On-premise applications (.NET, OWA, MOSS, etc)
    - Virtual Desktops
    - VPNs
  - Users/clients
    - Physically on network
    - Remote
    - Non-corporate assets
    - PC/Mac/Mobile

Identity Enforcement Platform

- Validate the user against her identity in THE directory
  - …wherever she is, on whatever client
  - …exceeding security requirements
  - …minimal user impact
- Pass authentication(s) to the application
  - …whatever the type of application
  - …staying fully compliant
  - …in the authentication protocol the application understands
  - …with the user ID the application wants

Identity translation

- SecureAuth IEP: on-premise
  - Store all IDs in the directory of record
  - Single "master" ID for all logins
  - Single store, full control and accountability
- Off premise, at application (or elsewhere)
  - Creates regulatory issues
  - Returns to spaghetti problem

Usage Scenarios

- Transparent access to Cloud from a Windows log-on
- Remote access with/without VPN
- Non-corporate assets, mobile devices
- Transient user base
- Mixed environments (multi-tenant cloud, traditional on-prem, private cloud, etc.) with different auth

Why IEP?

SecureAuth Enterprise Owned Authentication

1. **Central control/ownership of user store**
2. **Drop-in integration (no changing what is there)**
3. **Authentication configurable by application**
4. **Single point for Logging/Auditing**

How is it simpler?

- Reduces need for VPN licenses and network overhead for remote access
- Option for non-corporate assets
- No portal or proxy required
- Can integrate with access management solution– but no such requirement
- No token hardware or software to manage
- No provisioning/syncing of identities
- No change to schema, etc (no lock-in)
- Not tied to any single standard

How is it secure?

- Configurable 2-factor authentication
  - Bi-lateral, x509
  - Automated, out-of-band registration options
- SSO configurable by application
- Identity translations secure in directory
- Single point for logging/auditing

SecureAuth IEP

Come see SecureAuth in the Solution Center

Try Live Demos

Speak to Garret Grajek, SecureAuth CTO

ggrajek@multifa.com