

Mac Admin Casper LDAP

5-21-09



THE UNIVERSITY OF IOWA

Information Technology Services

Why LDAP lookup?

- Allows HawkID authentication
 - No need to keep track of an extra account
 - Enables activity logging
 - Enables group access & privilege control

Preparation

- Access to Active Directory tools
- Proper permissions to create and manage AD users and groups
- Create:
 - Casper service account
 - Casper privilege groups (admin, deploy...)
- Know:
 - Distinguished names of account, groups

LDAP Stuff

- More of an LDAP patch than an Active Directory integration
 - Several weaknesses
- Create account and groups
 - Microsoft Remote Server Administration Tools
- Look up DN for service account
 - Apache Directory Studio

Casper Connection Settings

Connection Search & Mappings

Display Name: UI AD

Scope: users

DNS Name or IP Address: iowadc1.iowa.uiowa.edu

Open/Close times out in: 15 seconds

Connection times out in: 60 seconds

☒ Use authentication when connecting

Authentication Type: Simple

Distinguished Name: CN=lst_casper_ldap,OU=S

Password:

☐ Encrypt using SSL

☐ Use custom port 389

Save LDAP Server

Casper Search & Mappings - Users

Connection Search & Mappings

Users

Map Users to ObjectClass values below

ObjectClass: (Comma separated)

Map User ID to:

Map Username to:

Map Real Name to:

Map Email Address to:

Append to email results:

Map Department to:

Map Building to:

Map Room to:

Map Phone to:

Map Position (Job Title) to:

Map Group Memberships to:

☒ Use Distinguished Name of groups

Search Base:

☒ all subtrees ☐ first level only

Casper Search & Mappings - Groups

User Groups

Map Groups to ObjectClass values below

ObjectClass: (Comma separated)

Map Group Name to:

Map Group ID:

Map Member Users to:

☒ Use Distinguished Name of members

Search Base:

☒ all subtrees ☐ first level only

Add Users & Groups – with a catch

- Users must be in the same AD OU
- Probably not an issue for single departments