IPICS LDAP User Import Configuration Example

November 8, 2016

Cisco Systems, Inc.
www.cisco.com

Cisco has more than 200 offices worldwide.
Addresses, phone numbers, and fax numbers are listed on the Cisco website at
www.cisco.com/go/offices.

IPICS LDAP User Import Configuration Example

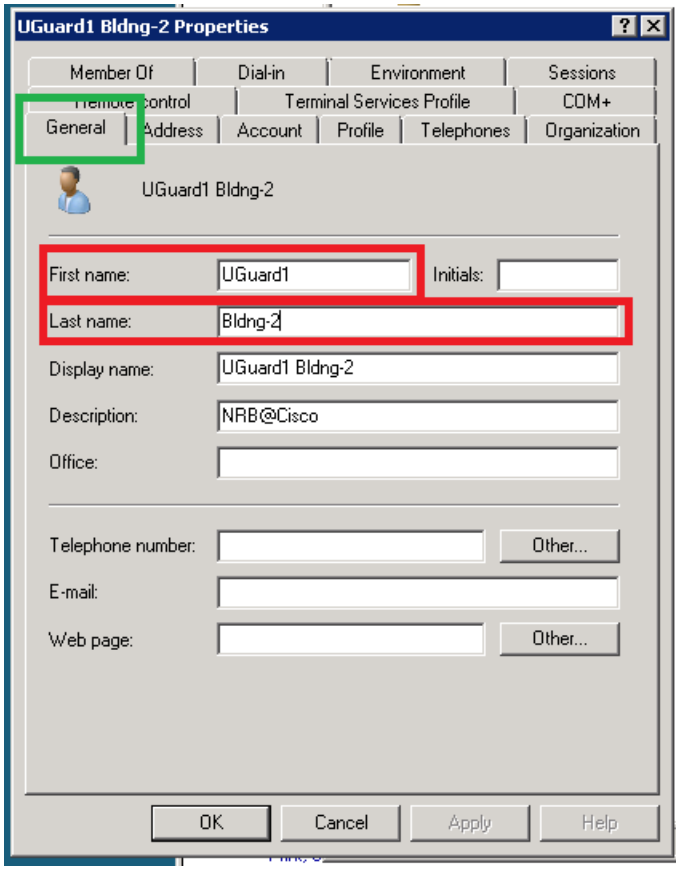
Version: This configuration example covers IPICS server version 4.6 or later

Configuration preparation: Create an LDAP user that has read-only access. This user will be defined in the LDAP User Import configuration settings on the IPICS server.

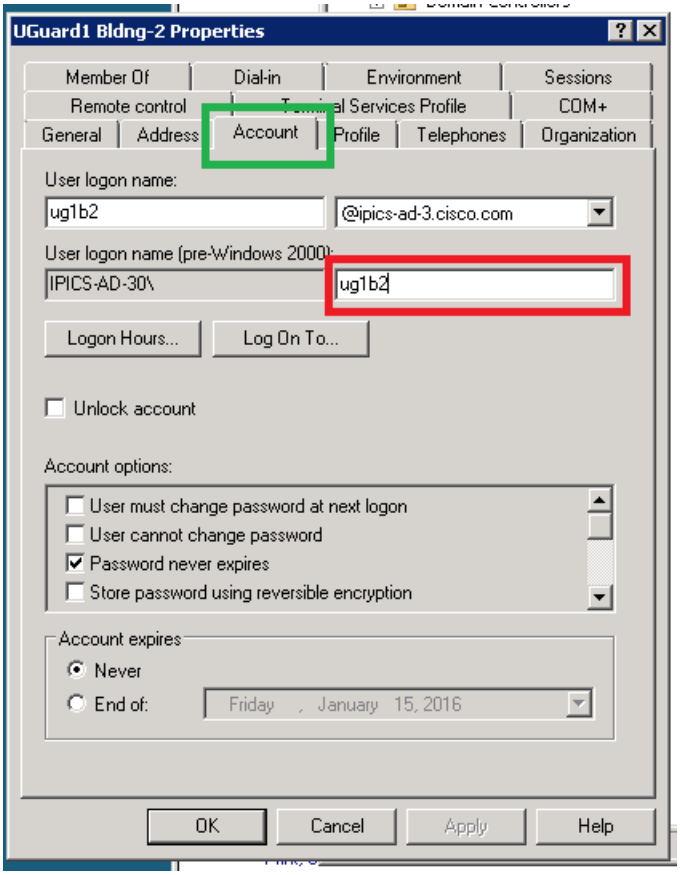
What fields are imported from Active Directory into IPICS?

The fields could be reviewed by running 'Active Directory Users and Computers' tool on the Windows Server.

1) User first name (GENERAL TAB, 'First name:' field)
2) User last name (GENERAL TAB, 'Last name:' field)



3) User login name (aka SAMAccountName, ACCOUNT TAB, the user ID that is to the right of the Windows domain field)



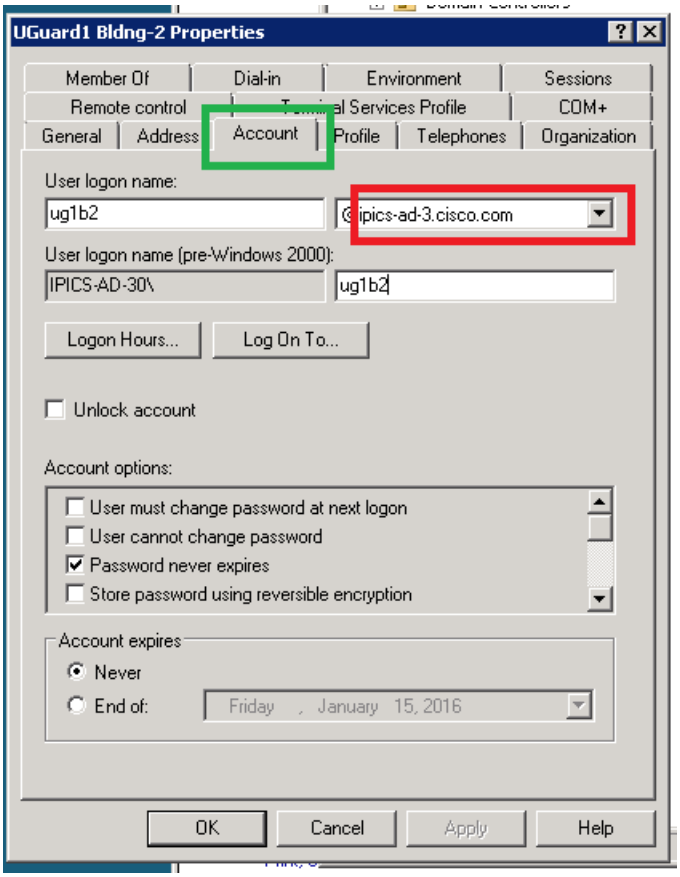
What fields are needed to configure LDAP User Import on the IPICS server?

On the IPICS server, the LDAP configuration parameters may be managed by running the import command with the "--ldapimport_config" flag. The corresponding fields could be reviewed by running 'Active Directory Users and Computers' tool on the Windows Server.

```
[ipicsadmin@ipics-esx19-vm1 ~]$ ipics_import_users --ldapimport_config
Please verify the current LDAP import settings:
-----------------------------------------------

Active Directory Domain Name : ipics-ad-3.cisco.com
LDAP Server Name             : 10.194.149.30
LDAP Server Port             : 389
LDAP Search Base             : cn=Users,dc=ipics-ad-3,dc=cisco,dc=com
LDAP Search Filter           : (&(objectClass=user))
Opsview to use               : ldap

LDAP Query User ID           : ldaptestuser
LDAP Query User Password     : ********

-----------------------------------------------

Would you like to change any of the value(s)?: (y/n)
```

a) Active Directory Domain Name : ipics-ad-3.cisco.com

This value is typically the domain name without the leading '@' character.



b) LDAP Server Name : 10.194.149.30

This value is the IP address or the DNS name of the Active Directory server.

c) LDAP Server Port : 389

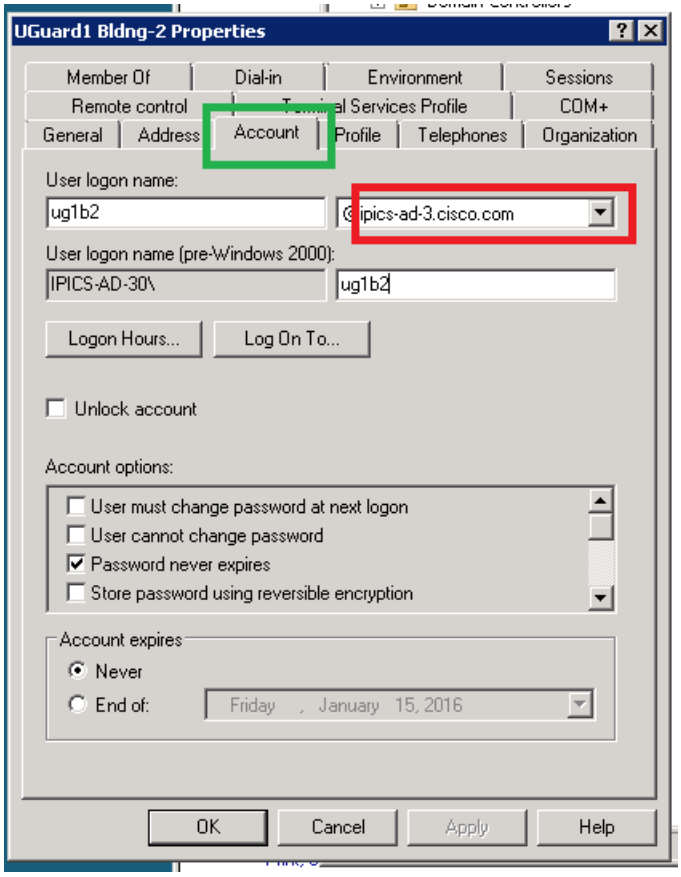
The standard Active Directory port is 389.

*Note: IPICS user authentication thru LDAP may use either secure/encrypted LDAP port, or standard non-encrypted port. However, IPICS user import supports non-encrypted LDAP port only at this time.

d) LDAP Search Base : cn=Users,dc=ipics-ad-3,dc=cisco,dc=com

This value indicates where in the LDAP tree should start searching for LDAP user records. While this is highly customizable, typical installation could just reformat the Active Directory domain name as follows:

AD Name	:	ipics-ad-3.cisco.com
Replace '.' With dc=…,	:	dc=ipics-ad3,dc=cisco,dc=com
Add 'cn=Users,' as prefix	:	cn=Users,dc=ipics-ad3,dc=cisco,dc=com

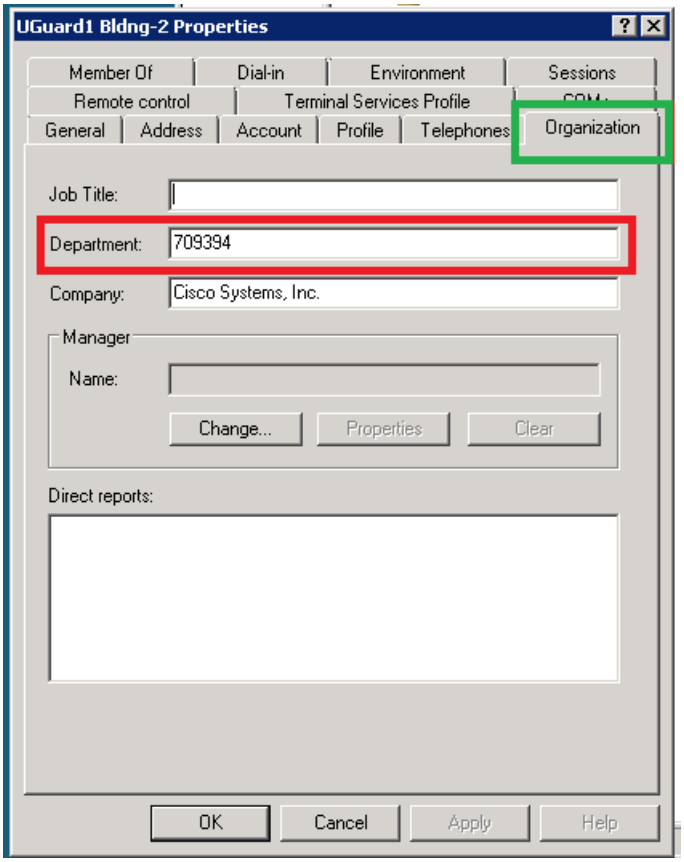


e) LDAP Search Filter : (&(objectClass=user))

While the search filter is highly customizable, typical installation may use "(&(objectClass=user))", which will include all user records as found in the LDAP tree (or sub-tree as specified by LDAP Search Base value above).

For example, if only a certain department should be included, the search filter may be changed to

(&(objectClass=user)(department=709394))



f) Opsview to use : ldap

This should be an existing Opsview defined in IPICS that has LDAP authentication enabled. All imported LDAP users would belong to this opsview.

g) LDAP Query User ID : ldaptestuser

This is a special Active Directory user who has read-only access in the Active Directory. This user should not have any administration privilege.

h) LDAP Query User Password : ********

The LDAP password for the special Active Directory user as defined in (g). This password is stored in IPICS in encrypted form. It is not synchronized: If the password is changed in the Active Directory, IPICS administrator must change this password on the IPICS server using --ldapimport_config' option.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2016 Cisco Systems, Inc. All rights reserved.