



ICE LDAP Configuration on ICE Server

Product guide for prerelease

Copyright © 2024, Instant Connect Software, LLC. All rights reserved.

Document version 1841, produced on Friday, September 06, 2024.

main 90adc8bf40040649230176bbdd465f6261a2d8e0

ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. STA GROUP DISCLAIMS ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL INSTANT CONNECT LLC OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF STA GROUP OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Trademarks mentioned in this document are the properties of their respective owners.

Contents

1 Document history	5
2 Introduction	5
3 LDAP system configuration	7
3.1 Search filter	9
3.2 AD Explorer: Find a search path	10
4 LDAP field mapping	10
4.1 Field mapping	11
5 LDAP service account	12
6 LDAP bulk import	12
7 Groups	13
8 Login with PIV smart card	14
9 Configure CA certificates for LDAP	17

List of Tables

1 Document history

Publication Date	Product Release	Notes
May 28, 2024	3.5.1	Added description for the 'Cache LDAP Credentials' feature.
April 15, 2024	3.5.0	Updated to reflect new ICE Desktop UI.
October 10, 2023	3.4.0	Updated examples for bulk and non-bulk import search filters.
September 28, 2023	3.4.0	Significant rewrite to better organize information. Added bulk import feature. Added group synchronization.
July 24, 2023	3.3.0	Updated ' <i>Complete AD LDS configuration on the ICE Desktop</i> ' and ' <i>Other Login Features</i> ' sections with new features and screenshots.
December 1, 2022	3.2.0	New release.
September 26, 2022	3.1.2	Release updates.
March 15, 2022	3.1.0	Document created.

2 Introduction

LDAP (Lightweight Directory Access Protocol) provides simplified, centralized resources and security administration for large organizations. ICE Server supports any LDAP service that allows authentication using email address, such as Microsoft Active Directory Lightweight Directory Services (AD LDS). The LDAP configuration information detailed below assumes the use of AD LDS, as it is the most commonly deployed LDAP solution.

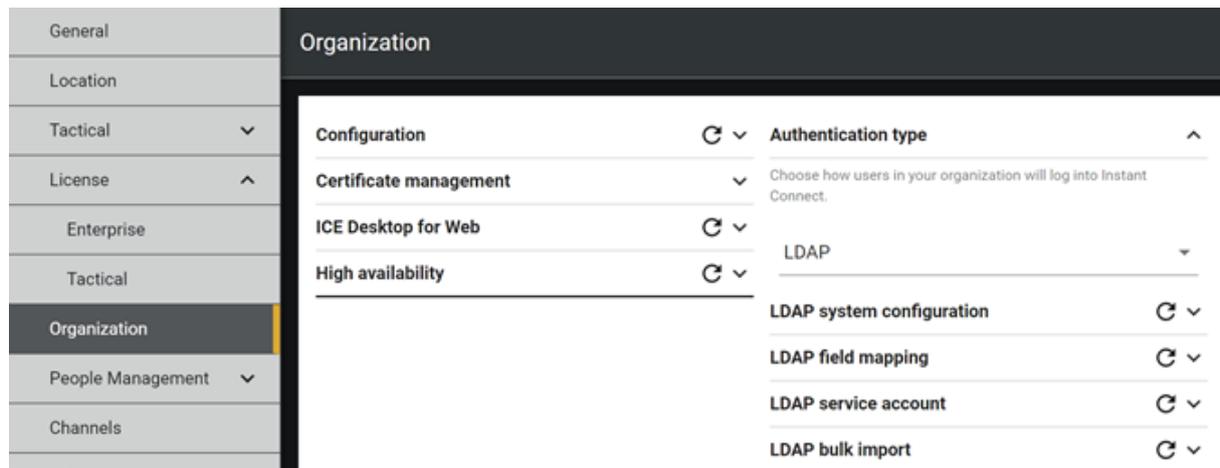
The supported versions of AD LDS are:

- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2

ICE LDAP Configuration on ICE Server

When enabled, users login to ICE Server using their AD email address (`userPrincipalName`). ICE users authenticated through AD LDS are assigned a standard user role on the ICE Server.

Begin by opening ICE Desktop and navigating to *Settings > Organization > Authentication type*. and select 'LDAP'. This adds the LDAP system configuration, field mapping, service account, and bulk import screens.



Note: Do *not* pre-create any user accounts on ICE Server which are meant to be managed thru LDAP user authentication! When a user logs into ICE Server for the first time using LDAP authorization, a standard ICE user account is automatically created for them. **After** that initial login and standard account creation, ICE admins may adjust the user role as needed, e.g., make them an admin user or workflow admin.

Note: We recommend using Microsoft Active Directory Explorer to browse your LDAP for mappable values. The following Active Directory values are inherited from LDAP, changes to these values must be done on the Active Directory server:

- First name
- Last name
- Password
- Display name
- Email address

3 LDAP system configuration

LDAP system configuration

When enabled, users logging into the system will be authenticated against this LDAP database, and their user record will be populated by specified fields.

Cache LDAP credentials

LDAP URL ldap://10.194.150.191:3268

Search base DC=cac-ad-2016,DC=icnow,DC=app

Search filter

```
(&(userPrincipalName=%s)
(memberOf=cn=ice3
Users,ou=ice2,ou=ice1,dc=exam
ple,dc=com))
```

UPN domain cac-ad-2016.icnow.app

Object	Description	Typical Value
Cache LDAP Credentials	When enabled, LDAP credentials will be stored locally and users will be authenticated against the cached credential whenever LDAP server cannot be reached. Note: This feature only works for users who have previously logged into ICE using a valid LDAP credential. It will not work for bulk-imported users who have not previously logged in.	
LDAP URL	Begins with either the <code>ldaps://</code> or <code>ldap://</code> protocol prefix, followed by the URL of the server responding to LDAP search requests. For <code>ldaps://</code> the server is communicating over an SSL connection.	For secure (SSL-enabled) LDAP: <code>ldaps://the active directory server name:636</code> (or 3269)For non-secure (non-SSL) LDAP: <code>.ldap://the active directory server name:389</code> (or 3268)
Search base	Defines the starting point for the search in the Active Directory tree.	Search base must be the top node of the AD tree for ICE Server users. All AD users who will be ICE Server users must belong to the same LDAP directory tree or sub-tree.
Search filter	Defines the LDAP query for searching users based on mapping of username to a particular LDAP attribute: <code>userPrincipalName</code> .	See the ‘Search filters’ section below.
UPN domain	The name of the Active Directory domain.	The value should be either the domain name of the Active Directory or an alternate UPN domain name. Note: ICE Server can only map to one <code>userPrincipalName</code> domain at a time.

3.1 Search filter

To understand a search filter, follow its path by reading it from right to left. The right-most component is the root of the tree, then follow the branch to the left-most component, which is the node (leaf) where the user will be found. For example, the following search filter...

```
(&(userPrincipalName=%s) (memberOf=cn=ice3 Users,ou=ice2,ou=ice1,dc=example,dc=com))
```

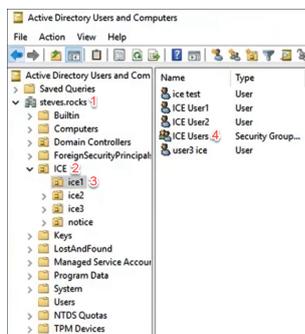
...can be read as:

- In Domain Component (DC)=com, find DC=example (the search base)
- In DC=example, find Organizational Unit (OU)=ice1
- In OU=ice1, find OU=ice2
- In OU=ice2, find the Common Name (CN)=ice3 Users
- In CN=ice3, find userPrincipalName=%s (the user)

Define a search filter to bulk import from multiple branches of the same search base using the following template:

```
(&(objectClass=person) ( | (memberOf=cn=ice3 Users,ou=ice2,ou=ice1,dc=example,dc=com) (memberOf=cn=iceb Users,ou=icea,ou=ice1,dc=example,dc=com) ) )
```

This is a visual example of another AD tree as displayed in AD Explorer:



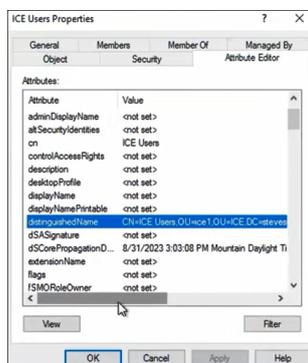
A search filter looking for a user in the ICE Users group, would look like this:

```
(&(userPrincipalName=%s) (memberOf=cn=ICE Users,ou=ice1,ou=ICE,dc=steves,dc=rocks))
```

1. steves.rocks: dc=steves,dc=rocks
2. ICE: ou=ICE
3. ice1: ou=ice1
4. ICE Users: memberOf=cn=ICE Users

3.2 AD Explorer: Find a search path

1. Within AD Explorer, navigate to a folder or object in the directory tree.
2. Right click on it.
3. From the resulting menu, select 'Properties'.
4. From the resulting 'Properties' screen, select the 'Attribute Editor' tab.
5. Scroll down the 'Attributes' list to the `distinguishedName` attribute.
6. The `distinguishedName` value provides the path which can be used to build the search filter.



4 LDAP field mapping

These fields comprise a list of LDAP attributes which must be mapped to the ICE Server user profile. While other LDAP attributes (either default, or custom) may be used for mapping, the typical values provided below are the most common ones and should work on most installations.

LDAP field mapping

Provide an LDAP query string to identify the field which it should be used to populate the Instant Connect user record.

First name

Last name

Alias

Username

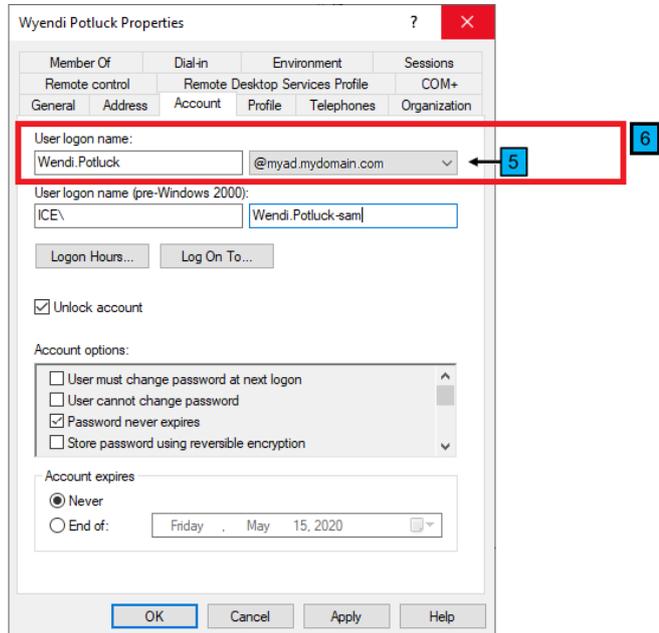
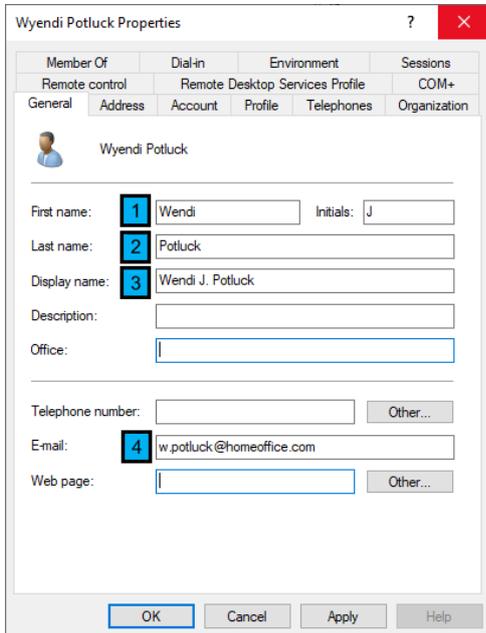
Object	Description	Typical Value
First name	The AD attribute for user first name.	<code>givenName</code>
Last name	The AD attribute for user last name.	<code>sn</code>

Object	Description	Typical Value
Alias	The AD attribute to be displayed in the ICE Server user profile. In AD LDS, <code>displayName</code> defaults to <code>givenName + initials + . + sn</code> .	<code>displayName</code>
Username	The AD attribute for user email address, which is used for login.	<code>userPrincipalName</code>

4.1 Field mapping

The screencaps below are presented as examples illustrating how LDAP fields are displayed in AD:

1. `givenName`
2. `sn`
3. `displayName`
4. `mail`
5. AD domain name
6. `userPrincipalName`



5 LDAP service account

This panel allows an admin to specify a 'service account' for ICE Server to use for accessing the LDAP or Active Directory systems. This feature is disabled (i.e., it has no affect) unless ICE Server is configured to authenticate users with LDAP. The primary uses for this feature are:

- For LDAP bulk import.
- For utilizing the 'Allow login with PIV card' feature and managing PIV identities via LDAP. ICE Server uses the service account specified here to access the LDAP directory and look for an account matching the identity of the PIV user (where the User Principal Name (UPN) is constructed as: `lastname.firstname.middlename.EDIPI@mil`). If such an account is found, the PIV user is logged in, otherwise their login is rejected.
- An LDAP system is configured such that a user does not have read access to their own LDAP record (an uncommon configuration). ICE Server uses the service account specified here to populate user information, e.g., first name, last name, email address.

LDAP service account

When enabled, use the supplied account credential to access the LDAP server for bulk import operations, CAC/PIV card access, or when using UPN subdomains.

Use service account when accessing LDAP

Username

Password

Object	Description
Use service account when accessing LDAP	Toggle on to enable the service account feature.
Username	The username for the service account on the LDAP server.
Password	The password for the service account on the LDAP server.

6 LDAP bulk import

Note: Requires an LDAP service account be configured.

Note: If a user is deleted from AD, they will still appear in ICE Desktop, but their login no longer works.

LDAP bulk import

Enable bulk import to create accounts for all LDAP users at once.
When disabled, user accounts are created only when the user first logs into Instant Connect.

Automatically run a bulk import each day

Search base

Search filter

Test execution

Object	Description
Automatically run a bulk import each day	Toggle on to enable a daily automatic import of LDAP users.
Search base	Defines the starting point for the search in the Active Directory tree. Search base must be the top node of the AD tree for ICE Server users. All AD users who will be ICE Server users must belong to the same LDAP directory tree or sub-tree.
Search filter	Defines the LDAP query for searching users based on mapping of username to a particular LDAP attribute: <code>objectClass=person</code> .
Bulk import now	Select this button to perform an import of LDAP users.
Test execution	Allows a test import of LDAP users, so that search base and search filter can be adjusted, if necessary.

Bulk import search filters target `objectClass=person`, instead of `userPrincipalName=%s`, otherwise they are structured the same as described in the 'Search filters' section above.

- Bulk import: `(&(objectClass=person) (memberOf=cn=ice3 Users,ou=ice2,ou=ice1,dc=example,dc=com))`
- Non-bulk: `(&(userPrincipalName=%s) (memberOf=cn=ice3 Users,ou=ice2,ou=ice1,dc=example,dc=com))`

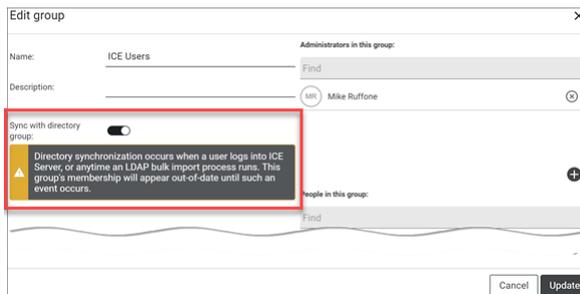
7 Groups

Note: If a user is deleted from AD, they will still appear in ICE Desktop, but their login no longer works.

ICE LDAP Configuration on ICE Server

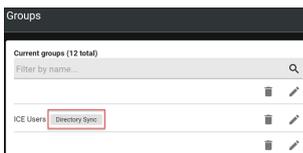
Group memberships can be synchronized from AD to ICE Desktop. One benefit is that users added to an AD group, once a data synch occurs, are also added to the corresponding ICE Desktop group *and* inherit any of that group's specifications, e.g., channel memberships.

For AD groups and ICE Desktop groups to remain in synch, data **must** flow from AD to ICE Desktop and **not** the other way. First create the AD group, then create the ICE Desktop group in the usual way, but with the following requirements:



Object	Description
Name	The group name entered here must exactly match the corresponding AD group name.
Sync with directory group	Must be toggled on.

These groups display in ICE Desktop with a 'Directory Sync' label. This is a visual reminder to **not** edit that group's name or members via ICE Desktop, as that **must** be done via AD.



8 Login with PIV smart card

On inserting a PIV smart card into an available smart card reader, the ICE Server desktop client login displays an additional 'Login with your Smart Card' option. This option is not visible if a PIV card is absent.

Instant Connect Enterprise Login

Instant Connect Enterprise Address

Username

Password

Login automatically

OR

Login with your Smart Card:
Connecting as: 1404767859113304@mil.

Enter pin code here

i You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only. By using this IS (which includes any device attached to this IS), you consent to the following conditions: -The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations. -At any time, the USG may inspect and seize data stored on this IS. -Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG-authorized purpose. -This IS includes security measures (e.g., authentication and access controls) to protect USG interests—not for your personal benefit or privacy. -Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

To enable this feature, go to Settings > Organization > Configuration and toggle on 'Allow login with PIV card'.

Configuration ↻ ^

Select whether users in your organization are allowed to login from multiple devices at the same time. Multiple logins consume multiple licenses. Choose how users in your organization can connect to ICE Server.

- Allow simultaneous logins
- Allow login with PIV card
- RTP/Multicast Failover
- Enable GIPHY in ICE Mobile

Require users to log in every	<input type="text" value="20"/>	days
Retain text messages for	<input type="text" value="5"/>	days
Retain text message attachments for	<input type="text" value="5"/>	days
Retain archived recordings for	<input type="text" value="5"/>	days
Retain ops log records for	<input type="text" value="5"/>	days

This feature requires the following:

1. A smart card reader attached to the relevant computer.

2. 'Login with PIV smart card' enabled via 'Organization' screen, otherwise attempts to read the PIV smart card will fail.
3. The user's ICE Server username must be `CommonName@OrganizationalUnit`
 - `CommonName` and `OrganizationalUnit` correspond with the fields of the same name on the user's PIV profile, which is read by the smart card reader.
 - Multiple values for `OrganizationalUnit` are concatenated for the ICE Server username.
4. The smart card reader must be able to read the inserted PIV smart card.

To login with a PIV smart card:

Note: The 'Login automatically' function has no affect on login with a PIV smart card.

1. Enter server address.
2. Insert smart card. The 'Login with your Smart Card' option will display.
3. Select 'Login with Smart Card'.

9 Configure CA certificates for LDAP

Please refer to the *ICE Server Installation Guide* for instructions on accessing the 'ICE OS Configuration Wizard' and configuring the CA certificates used for LDAP. By default, the system certificates are also used for LDAP, but that can be disabled, allowing for LDAP-specific CA certificates to be configured, too (see the 'TLS Certs' screen of the configuration wizard).