OVERVIEW

IP*edge* Enterprise Manager Active Directory Sync (ADSync) is a feature that automatically configures telephone users in the IP*edge* system based on data entry in the Active Directory service.

- Active Directory Sync is a menu in Enterprise Manager. No external application is necessary.
- It supports manual and scheduled approaches.
- It supports Microsoft Active Directory (AD) service and OpenLDAP service.
- ADSync only reads data from Active Directory service but does not write data to the Active Directory.
- Any change made in IP*edge* is not propagated to AD.
- When there is a new entry in AD, a new user is created based on the AD and ADSync settings and default settings for the telephone in the IP*edge* system.
- If a user is deleted from AD, an entry in IP*edge* is removed or disabled based on setting in the ADSync.
- In case of manual synch, all the changes are shown, and information can be edited before applying changes.
- Unattended Synch can be scheduled. The scheduler uses Linux CronTab.
- Items to be synced are Name, DN, User ID and email for UM.
- Enterprise Manager Personal Administration (EMPA) is able to login using AD authentication when AD authentication is enabled.
- Multi-node IP*edge* systems are supported. The node is identified by the specified key field and key value.
- When applying changes (including auto synch with schedule), an application check box is shown. If it is selected, the user is created for the application. Applications will be EMPA and Messaging.
- One user/password authenticated by AD can login to EMPA and Voicemail. But to login to Voice Mail from a telephone requires a separate password.
- ADSync will not create an Enterprise Manager administration account or user. AD authentication does not apply to Enterprise Manager administration user.
- An AD user account must have a valid phone number in the designated phone attribute in order to be queried.
- An AD user which does not have a phone number is excluded from this process.

Active Directory Synchronization (AD sync)

IP*edge* Active Directory Synchronization (AD sync) allows an administrator to import user information such as the name and telephone number to the IP*edge* system. It makes it easy for an administrator to install the new system by importing the user information from the existing Active Directory. It can also be used to automatically import changes such as new users, deleted users, and modifying existing users by scheduling synchronization.

AD sync supports networked IP*edge* systems, and users can be assigned to the proper IP*edge* system based on the value of the specified data field such as Office in the Active Directory.

Active Directory Sync also supports LDAP server.

Active Directory Sync

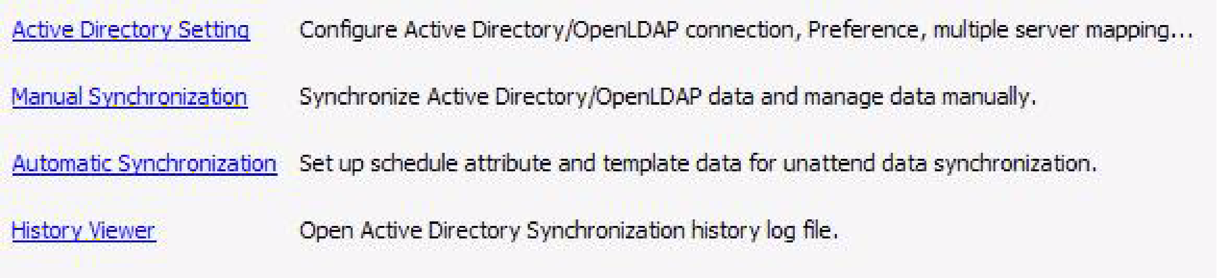
Operation - Not applicable. See PROGRAMMING section.

PROGRAMMING

Active Directory Synch

Click on **Station > Active Directory Sync**.

The various configuration options screen displays (shown below).



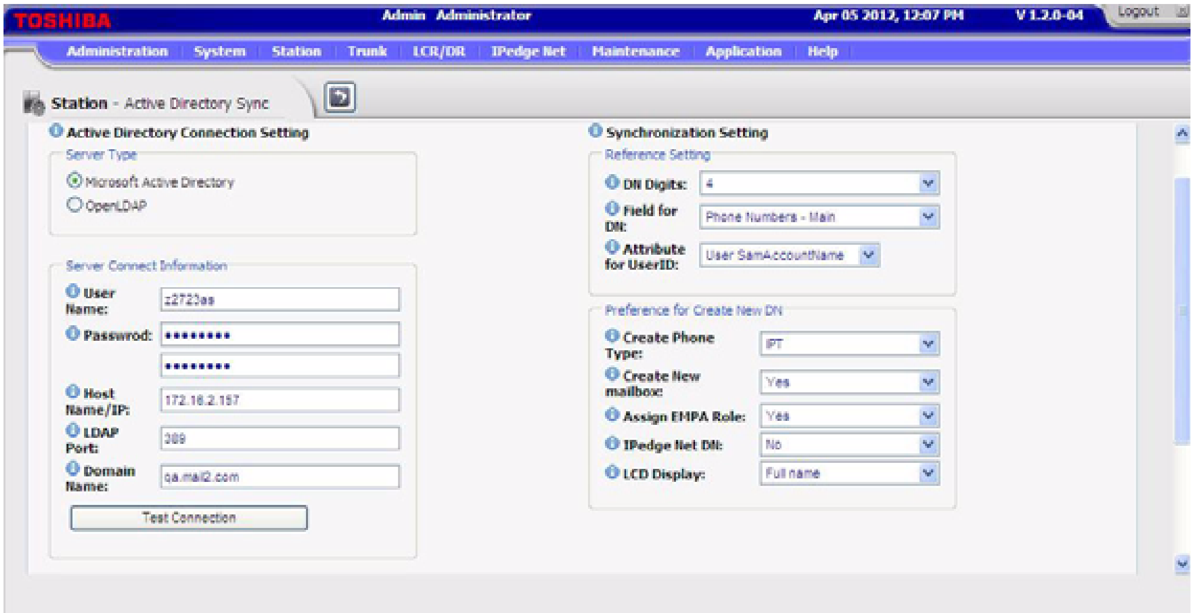
Active Directory Setting	Configure Active Directory/OpenLDAP connection, Preference, multiple server mapping...
Manual Synchronization	Synchronize Active Directory/OpenLDAP data and manage data manually.
Automatic Synchronization	Set up schedule attribute and template data for unattend data synchronization.
History Viewer	Open Active Directory Synchronization history log file.

Active Directory Settings

The administrator will need to provide AD Administrator information in order to enable the IP*edge* to connect to the Active Directory service. The AD connection must be pre-configured in order for Enterprise ADSync to perform the data synchronization.

The connect information is saved in Enterprise Manager database and use by both manual and unattended schedule.

Enterprise Manager provides a [Test Connection] button to verify the connection to the Active Directory (shown below).



TOSHIBA
Admin Administrator
Apr 05 2012, 12:07 PM
V 1.2.0-04
Logout
Administration | System | Station | Trunk | LCR/DR | IPedge Net | Maintenance | Application | Help

Station - Active Directory Sync

Active Directory Connection Setting

Server Type

● Microsoft Active Directory

○ OpenLDAP

Server Connect Information

User Name: z2723as

Passwrod: ********

****

Host Name/IP: 172.16.2.157

LDAP Port: 389

Domain Name: qa.mail2.com

Synchronization Setting

Reference Setting

DN Digits: 4

Field for DN: Phone Numbers - Main

Attribute for UserID: User SamAccountName

Preference for Create New DN

Create Phone Type: IPT

Create New mailbox: Yes

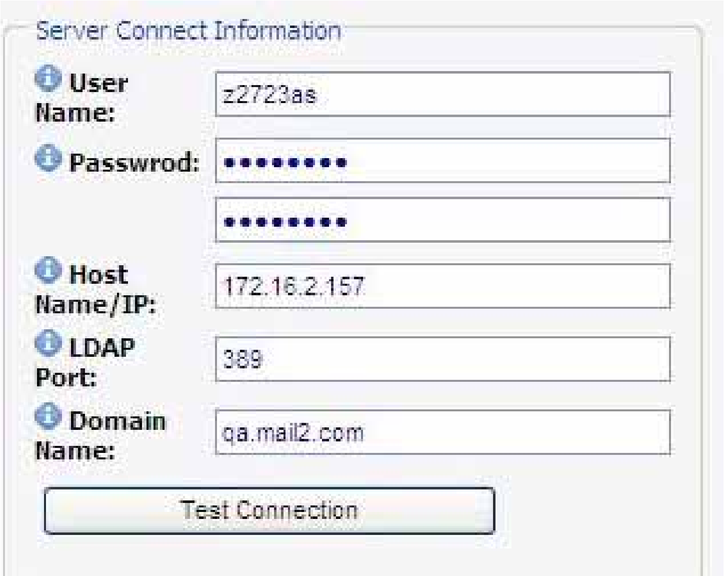
Assign EMPA Role: Yes

IPedge Net DN: No

LCD Display: Full name

To connect to AD Service user needs to provide AD Administrator information, such as, User Name, Password, AD Server IP address, LDAP port and Domain Name (shown below).

Default port is 389.



Server Connect Information

User Name: z2723as

Passwrod: ••••••••

••••••••

Host Name/IP: 172.16.2.157

LDAP Port: 389

Domain Name: qa.mail2.com

When Enterprise Manager ADSync successfully connects to AD service a screen with “Your connection has been verified” displays.

If Enterprise Manager could not locate or connect to the AD service, then the following message displays “Connection: Failed...”.

If AD service is connects but authentication fails or other error reports by AD, and then the AD error message displays.

AD Authentication

The User created by ADSync has the capability to authenticate using AD server for accessing Enterprise Manager Personal Edition.

Authentication mode can be set to

- Use only Enterprise Manager authentication – Enterprise Manager uses the DN as the User ID.
- Use only AD authentication – uses the AD user name and password to login.
- Use both IP*edge* and AD Authentication – Uses either DN or AD user name to access Enterprise Manager Personal Administrator. The AD user password is never synchronized nor saved to Enterprise Manager database. Thus when AD user password is changed by the AD administrator, the EMPA user needs to apply the new password. If the password expiration is enabled, the new password must be set from Windows or Microsoft applications.

Integration Configuration

Synchronization Settings

Enterprise Manager administrator must specify the number of digits to be used for a Prime DN in the IP*edge* server. A Prime DN can be from 3 to 10 digits in length.

ADSync uses telephone number stored in AD fields “telephonenumber” or “ipPhone”. Only one field can be specified for a system/enterprise.

If user has more than one telephone number defined in AD, the main telephone number will be used.

Preferences to create New DN

For parameters that are not in AD but are used for user creation can be specified in Active Directory Setting page.

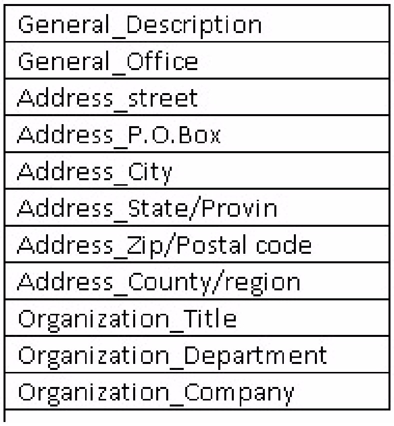
The setting will be used for both Manual synch and Automatic synch. Manual synch lets the user modify or override the preset parameters individually.

- Phone Type – Default value can be IPT telephone or SIP telephone.
- Create Mailbox – A mailbox will be created for the new user.
- Assign EMPA – Personal Admin (as know as EMPA) will be created for this user or not.
- IP*edge* Net DN – In IP*edge* Net DN case, the DN will be propagated to all Network DN tables in the IP*edge* Net servers.
- IP Phone LCD name display – Administrator has the option to select the phone display content from the AD Full Name attribute, Display Name attribute or assembled from FirstName and LastName combinations.

Multiple-Node Support

To distinguish the AD users belonging to different IP*edge* nodes, a key field in AD can be specified.

The AD key field can be used are:



General_Description
General_Office
Address_street
Address_P.O.Box
Address_City
Address_State/Provin
Address_Zip/Postal code
Address_County/region
Organization_Title
Organization_Department
Organization_Company

The values designated to an IP*edge* node are also defined in Enterprise Manager server database.

If member server is detected by Enterprise Manager then the Multiple Server Setting section displays. If member is attached then the Key Field is mandatory.

The value can be text or number. If Key Field Value is blank then no user will be created to this node.

If a Key value in AD does not match to any server key value then the user will be recorded in the conflict report.

New AD Entry

When a DN does not exist in the IP*edge* system, it is treated as a New User.

Predefined settings apply to all new users.

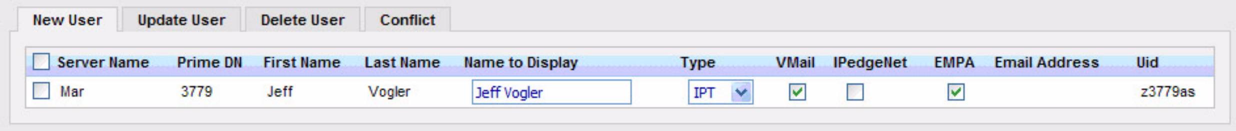
When an automatic sync is performed, a DN with the predefined phone type will be created in the IP*edge* system; a matching Voice Mail box and EMPA user can also be created if predefined. All Network DN tables can be updated if predefined.

If a DN already exists in the target IP*edge* server, then the AD data overrides the current Display Name.

In manual case, the predefined setting will be checked and presented to the user for editing.

New user will be created when the checkbox is checked. Default the user is unchecked.

User can edit Name to Display, Phone Type, Voice Mail box, EMPA and IP*edge* Net option.



□	Server Name	Prime DN	First Name	Last Name	Name to Display	Type	VMail	IPedgeNet	EMPA	Email Address	Uid
□	Mar	3779	Jeff	Vogler	Jeff Vogler	IPT	☑	□	☑		z3779as

If the DN already exists in the target IP*edge* server, then Enterprise Manager examines the display name. If display name does not match then this user appears in Update category, otherwise it is ignored.

If the display name does not match, it is dropped in the Conflict category.

The Phone user creation follows the same rules of a normal station creation in the Enterprise Manager Station Assignment. Such as ADSync does not pre-screen for Network DN table conflict. Errors will be reported in the log.

Note: ADSync does not scan AD data for potential failure condition such as two AD users having the same last four digits in their telephone number.

Update User

When DN exists but User ID is not the same, DN will be in the Update User group. The conflicting data is for informational purposes only.

When users last name or first name has changed, DN will be in the Update User group.

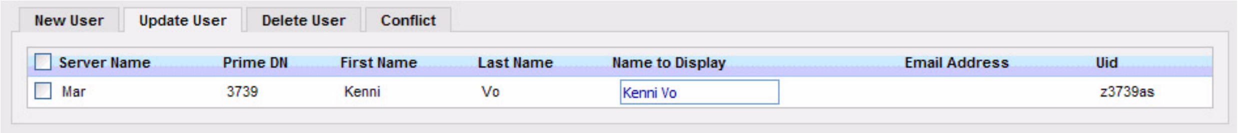
If the Display Name is overwritten by the administrator using Enterprise Manager then it will not show in the Update category until the name is changed in AD.

Silent Update – When Enterprise Manager detects an existing PDN is running sync the first time, an AD user sync record will be added.

If the telephone user has EMPA enabled then after updating, the user will be able to login using the UID if it is applicable.

Update will not override the current EMPA, IP*edge* Net or voice mailbox settings for an existing DN.

In the manual step, the only field that can be edited is the Display Name.



□ Server Name	Prime DN	First Name	Last Name	Name to Display	Email Address	Uid
□ Mar	3739	Kenni	Vo	Kenni Vo		z3739as

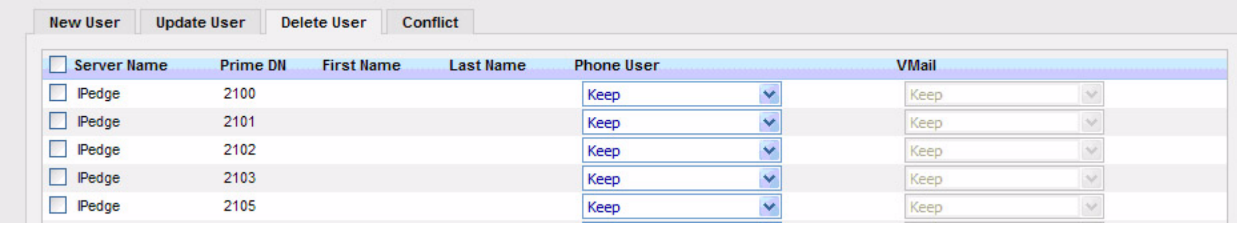
To update the change, the checkbox must be checked.

Delete User

When a DN exists in the IP*edge* server but not in AD, data will be put in the Delete User category.

In manual sync, a user in the Delete User category has the option to keep the user, disable the port or delete the user from the server. A deleted user can also have the option to keep or delete the voice mailbox.

In the case of automatic sync, a user is not deleted automatically. The Administrator can preselect to Ignore or Disable the port. To permanently remove the DN from the server, the administrator must use the Station Assignment page.



□ Server Name	Prime DN	First Name	Last Name	Phone User	VMail
□ IPedge	2100			Keep	Keep
□ IPedge	2101			Keep	Keep
□ IPedge	2102			Keep	Keep
□ IPedge	2103			Keep	Keep
□ IPedge	2105			Keep	Keep

Conflict User

Users in the Conflict category will be displayed at beginning of the user management page.

Enterprise Manager does not try to resolve the conflicts nor does it provide a tool to resolve conflicts.

A user can either correct the problem and run AD Sync again or ignore the conflict and continue the rest of the integration.

Possible reasons for a conflict include:

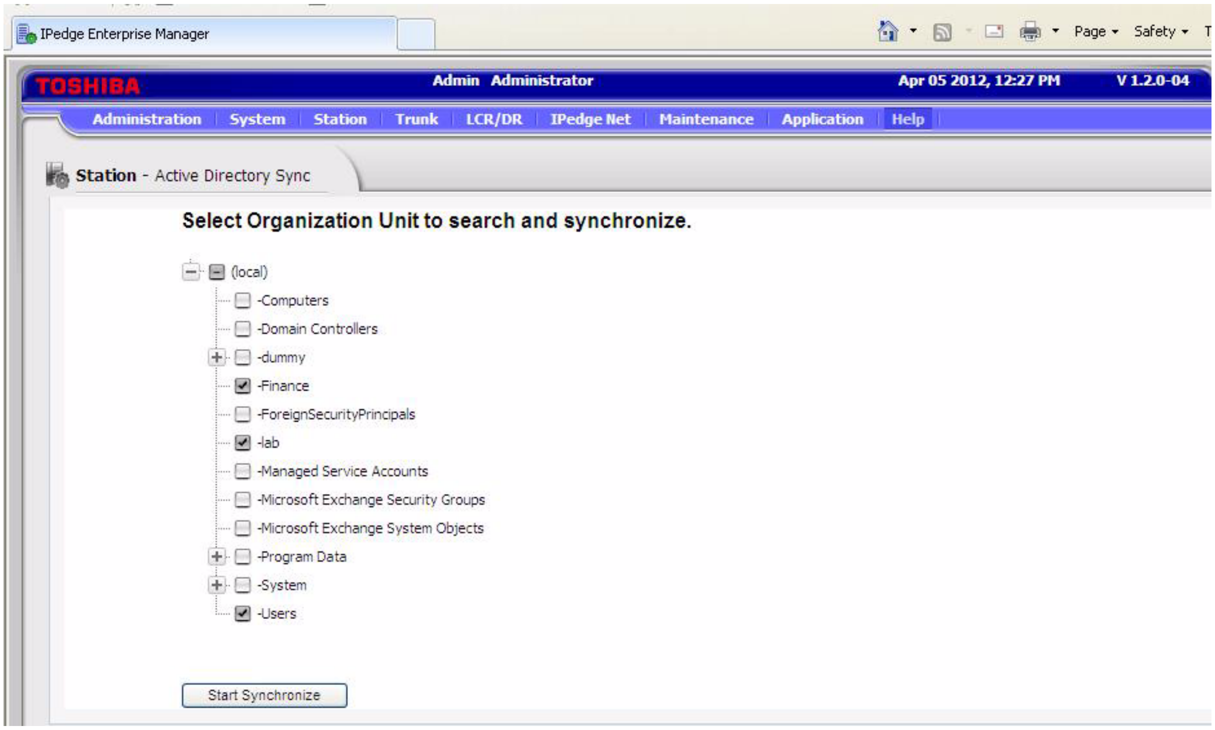
- In a multiple server environment, a new user is missing the Group Key field value. AD Sync could not determine which IP*edge* system to assign the user to.
- When AD Authentication is applied, the same User ID appears for multiple DNs.
- The user ID already exists, but the DN is not the same.
- The user ID exists and the DN is the same, but IP*edge* server node is not same.

In automatic synch, the conflict user is logged in the report file.

Manual Synch

Using Manual Synch you can select which organization unit(s) to be synchronized. The administrator also can review and modify entries before synchronizing the data in the IP*edge* server.

When manual synch is chosen, Enterprise Manager connects to the AD Service and collects the organization unit data. Users can view the tree hierarchy built (shown below) by Enterprise Manager that is similar to the folder TreeView in the Active Directory Administrative Center.



Select Organization Unit to search and synchronize.

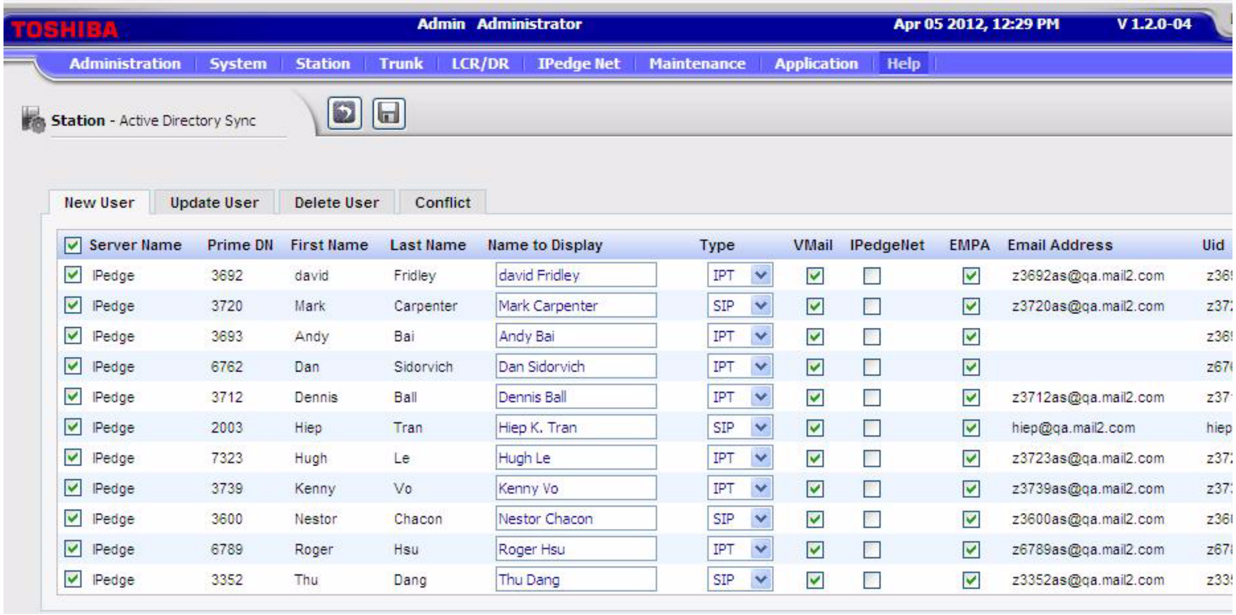
- ▣ (local)
  - □ -Computers
  - □ -Domain Controllers
  - □ -dummy
  - ☑ -Finance
  - □ -ForeignSecurityPrincipals
  - ☑ -lab
  - □ -Managed Service Accounts
  - □ -Microsoft Exchange Security Groups
  - □ -Microsoft Exchange System Objects
  - □ -Program Data
  - □ -System
  - ☑ -Users

When you click Start Synchronize, the following screen displays.

Check the box next to Server Name to select all or check appropriate boxes individually.

You can also change the type of station to either IPT or SIP using the drop down in the type column.

Click the Save icon after making the appropriate changes.



☑ Server Name	Prime DN	First Name	Last Name	Name to Display	Type	VMail	IPedgeNet	EMPA	Email Address	Uid
☑ IPedge	3692	david	Fridley	david Fridley	IPT	☑	□	☑	z3692as@qa.mail2.com	z36
☑ IPedge	3720	Mark	Carpenter	Mark Carpenter	SIP	☑	□	☑	z3720as@qa.mail2.com	z37
☑ IPedge	3693	Andy	Bai	Andy Bai	IPT	☑	□	☑		z36
☑ IPedge	6762	Dan	Sidorvich	Dan Sidorvich	IPT	☑	□	☑		z67
☑ IPedge	3712	Dennis	Ball	Dennis Ball	IPT	☑	□	☑	z3712as@qa.mail2.com	z37
☑ IPedge	2003	Hiep	Tran	Hiep K. Tran	SIP	☑	□	☑	hiep@qa.mail2.com	hiep
☑ IPedge	7323	Hugh	Le	Hugh Le	IPT	☑	□	☑	z3723as@qa.mail2.com	z37
☑ IPedge	3739	Kenny	Vo	Kenny Vo	IPT	☑	□	☑	z3739as@qa.mail2.com	z37
☑ IPedge	3600	Nestor	Chacon	Nestor Chacon	SIP	☑	□	☑	z3600as@qa.mail2.com	z36
☑ IPedge	6789	Roger	Hsu	Roger Hsu	IPT	☑	□	☑	z6789as@qa.mail2.com	z67
☑ IPedge	3352	Thu	Dang	Thu Dang	SIP	☑	□	☑	z3352as@qa.mail2.com	z33

Note: Check Station > Station Assignments to verify the newly created DNs.

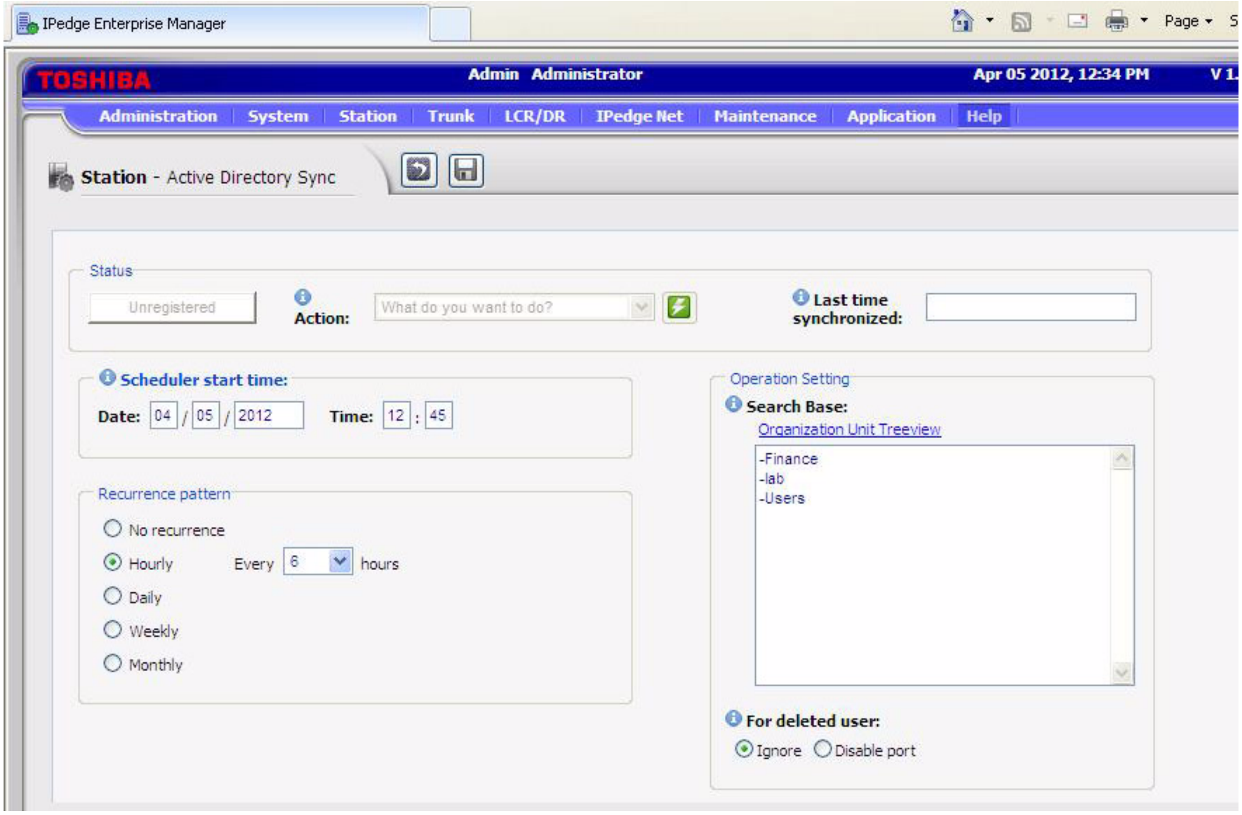
Automatic Synch

ADSync can be configured to run unattended based on preset parameters and conditions (shown below).

The Active Directory Settings described above apply to both Manual Synch and Automatic Synch. There are some settings that only apply to the unattended operation.

The unattended operation can be scheduled repeatedly or just once. The scheduled events can be suspended, resumed or cancelled.

The result is an XML format log file. The Administrator can view or print the file from the History Viewer.



Station - Active Directory Sync

Status

Unregistered

Action: What do you want to do?

Last time synchronized:

Scheduler start time:

Date: 04 / 05 / 2012 Time: 12 : 45

Recurrence pattern

○ No recurrence

● Hourly Every 6 hours

○ Daily

○ Weekly

○ Monthly

Operation Setting

Search Base: Organization Unit Treeview

-Finance
-lab
-Users

For deleted user: ● Ignore ○ Disable port

Schedule recurrence events

The Automatic Synch can be set up as recurring events to one time only, every x hour, every x day, every day of the week or every month.

Schedule Start Time: The Start Date and Time is the initial time set for scheduler to start. Once the scheduler has begun and the initial date and time has passed, the field will be blank.

Recurrence Patterns:

No recurrence – can be set to run once at this time or can be set for a future time to synch.

Hourly – The minimum time set can be from 6 hours to a maximum of 23 hours from the Start Time. The synch will run at the Start Date and Time, and recurring every x hour after. This is to avoid system performance overhead.

Daily – Allow set from 1 ~ 31. ADSynch will be executed every x day from the initial Start Date. The execution time is the Start Time that is initially set.

Weekly – Specifies a day of the week to execute the synchronization. If the start date does not match the day of the week supplied then sync will run on the next matching day of the week. For example, if the schedule is set to every Wednesday and Start Date is 1/24, which is Tuesday. The scheduler will start on 1/24, but the first synch will run on 1/25. The execute time is the Start Time that is initially set.

Monthly – Unit from 1 – 12. The recurring will be same date of the x month duration. For example, initial Start Date is 1/24 and every one month. The recurring date will be 1/24, 2/24, 3/24 …etc. If a date set 30, 31 or 29 for leap month then event gets ignored.

Pre-setting

AD Sync does not delete a user unattended. The administrator must login with Enterprise Manager and delete it from Station Assignments. If AD Sync detects a user has been deleted from AD then Enterprise Manager can either disable the IP port or ignore the change.

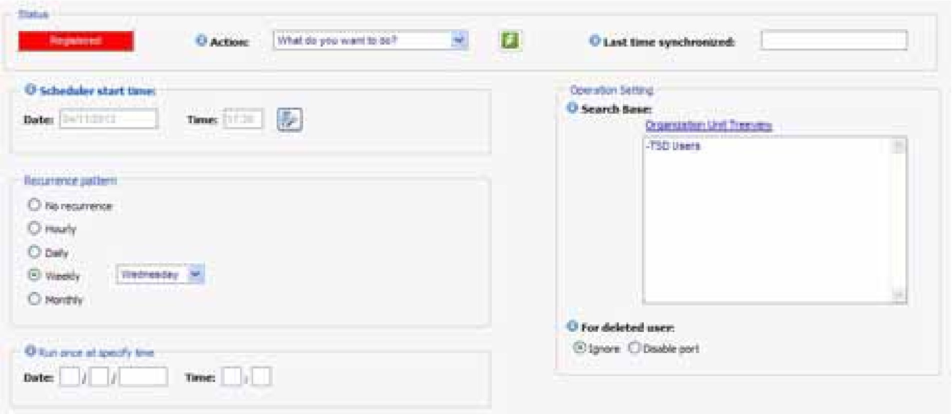
AD Sync search base field is mandatory. This field is not editable. The User must use the Organization Unit Treeview to get the current data from the AD server.

Scheduler Control

When the administrator saves the data in the page, the scheduler automatically starts.

Scheduler status displays. User can temporary suspend the scheduler being executing an action, resume paused scheduler or cancel scheduler and remove all events.

AD Sync enables the administrator to set up a single unattended execution without interrupt the recurring events. The information will display when the event has not be executed. Once the event is executed the data will be removed.



Status

Registered

Action: What do you want to do?

Last time synchronized:

Scheduler start time:

Date: 04/11/2012 Time: 17:30

Recurrence pattern

○ No recurrence
○ Hourly
○ Daily
● Weekly Wednesday
○ Monthly

Run once at specify time

Date: □ / □ / □ Time: □ : □

Operation Setting

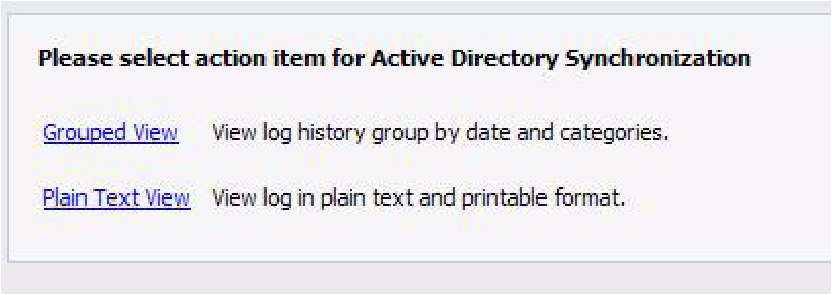
Search Base: Organization Unit Treeview

-TSD Users

For deleted user: ● Ignore ○ Disable port

History Viewer

All AD Sync results are recorded into an XML formatted file. Enterprise Manager provides the History View to view the recorded data. The recorded data is presented in an intuitive readable format. The user can view records by date and other categories. The entire log file can be printed from the Web.



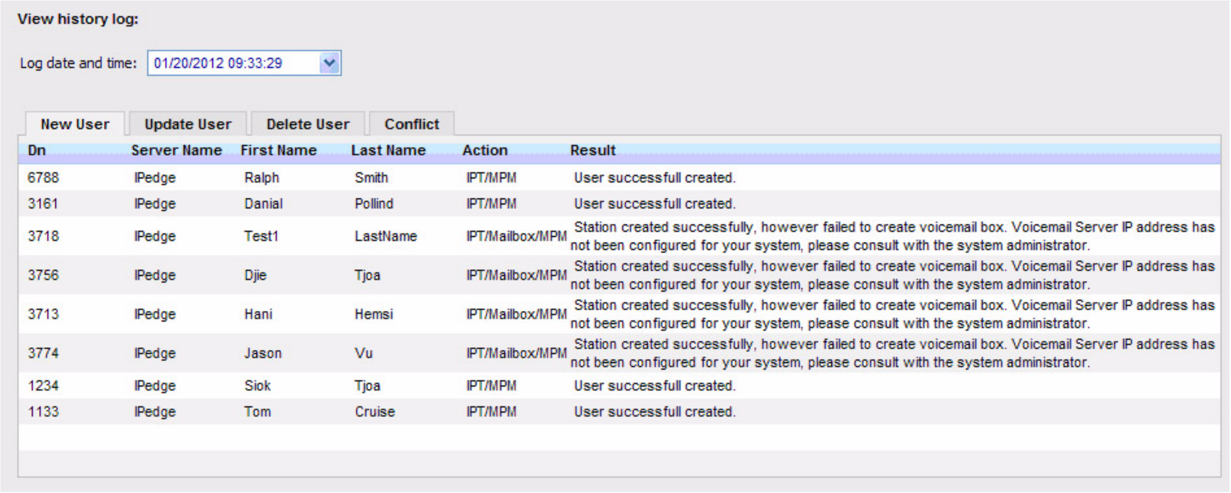
Please select action item for Active Directory Synchronization

Grouped View — View log history group by date and categories.

Plain Text View — View log in plain text and printable format.

Grouped View

The log data is organized into New User, Update User, Delete User and Conflict categories (tabs shown below). Data are sorted by date and time.



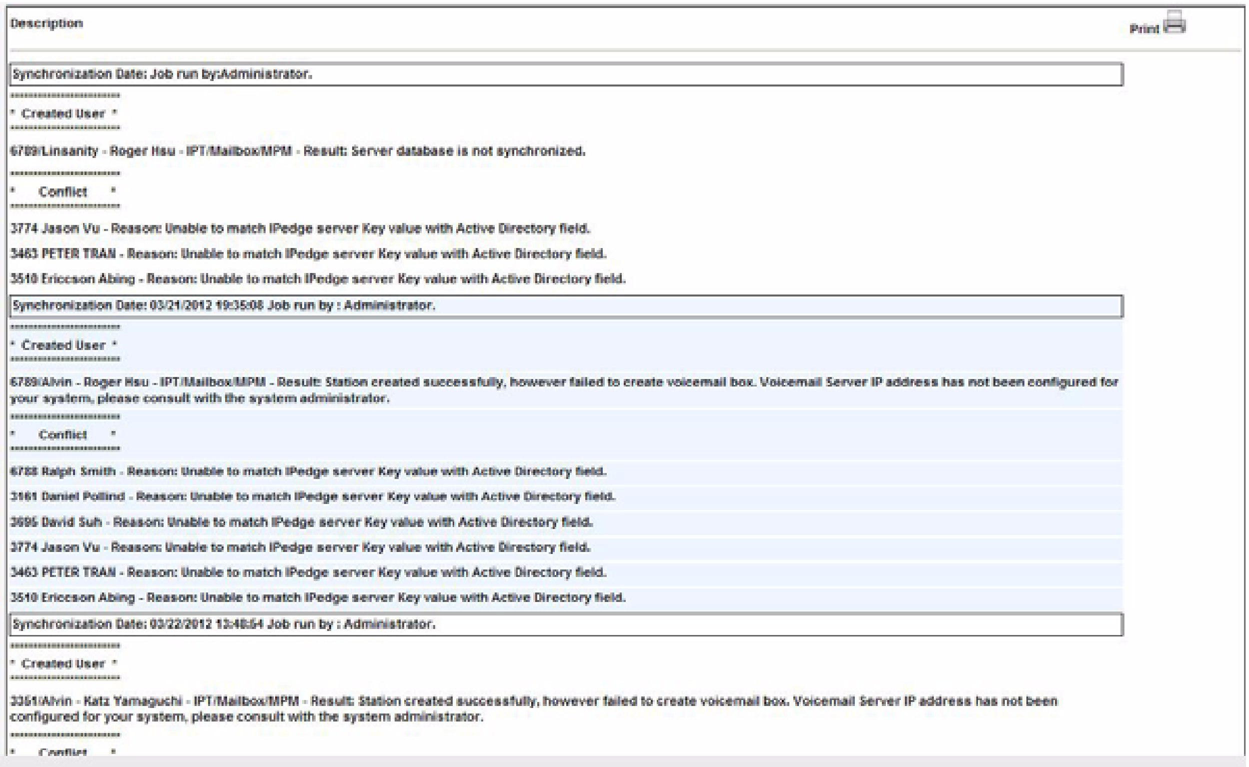
View history log:

Log date and time: 01/20/2012 09:33:29

Dn	Server Name	First Name	Last Name	Action	Result
6788	IPedge	Ralph	Smith	IPT/MPM	User successfull created.
3161	IPedge	Danial	Pollind	IPT/MPM	User successfull created.
3718	IPedge	Test1	LastName	IPT/Mailbox/MPM	Station created successfully, however failed to create voicemail box. Voicemail Server IP address has not been configured for your system, please consult with the system administrator.
3756	IPedge	Djie	Tjoa	IPT/Mailbox/MPM	Station created successfully, however failed to create voicemail box. Voicemail Server IP address has not been configured for your system, please consult with the system administrator.
3713	IPedge	Hani	Hemsi	IPT/Mailbox/MPM	Station created successfully, however failed to create voicemail box. Voicemail Server IP address has not been configured for your system, please consult with the system administrator.
3774	IPedge	Jason	Vu	IPT/Mailbox/MPM	Station created successfully, however failed to create voicemail box. Voicemail Server IP address has not been configured for your system, please consult with the system administrator.
1234	IPedge	Siok	Tjoa	IPT/MPM	User successfull created.
1133	IPedge	Tom	Cruise	IPT/MPM	User successfull created.

Plain Text View

In this view, Enterprise Manager retrieves log data and formats the data into readable plain text format. There is a [Print] icon which can print all the content.



```
Synchronization Date: Job run by:Administrator.
************************
* Created User *
************************
6789/Linsanity - Roger Hsu - IPT/Mailbox/MPM - Result: Server database is not synchronized.
************************
*     Conflict     *
************************
3774 Jason Vu - Reason: Unable to match IPedge server Key value with Active Directory field.
3463 PETER TRAN - Reason: Unable to match IPedge server Key value with Active Directory field.
3510 Ericcson Abing - Reason: Unable to match IPedge server Key value with Active Directory field.
Synchronization Date: 03/21/2012 19:35:08 Job run by : Administrator.
************************
* Created User *
************************
6789/Alvin - Roger Hsu - IPT/Mailbox/MPM - Result: Station created successfully, however failed to create voicemail box. Voicemail Server IP address has not been configured for
your system, please consult with the system administrator.
************************
*     Conflict     *
************************
6788 Ralph Smith - Reason: Unable to match IPedge server Key value with Active Directory field.
3161 Daniel Pollind - Reason: Unable to match IPedge server Key value with Active Directory field.
3695 David Suh - Reason: Unable to match IPedge server Key value with Active Directory field.
3774 Jason Vu - Reason: Unable to match IPedge server Key value with Active Directory field.
3463 PETER TRAN - Reason: Unable to match IPedge server Key value with Active Directory field.
3510 Ericcson Abing - Reason: Unable to match IPedge server Key value with Active Directory field.
Synchronization Date: 03/22/2012 13:48:54 Job run by : Administrator.
************************
* Created User *
************************
3351/Alvin - Katz Yamaguchi - IPT/Mailbox/MPM - Result: Station created successfully, however failed to create voicemail box. Voicemail Server IP address has not been
configured for your system, please consult with the system administrator.
************************
*     Conflict     *
```

Log file rolling

The log file is in xml format named AdSyncLog.xml. If the file size reach the maximum size of 10M then it rolls to AdSyncLog1.xml and starts a new AdSyncLog.xml. The file only rolls one version.

Other Application Sync

Enterprise Manager Personal Administration (EMPA)

An EMPA user may be created according to the ADSync preference setting or manual setting selected.

If EMPA creation is selected, user last name, first name, uid and email from AD are stored for the EMPA user.

If AD authentication is enabled, EMPA user that is able to log in uses AD user name and password.

EMPA user that is created from Enterprise Manager does not have the AD authentication capability.

Messaging

The user is able to login into IP*edge* Messaging from EMPA uses the AD name and password. If the user is accessing the mailbox via a telephone, they are required to use the mailbox password.

Other Directory Service Support

Enterprise Manager ADSync also supports LDAP/OpenLDAP

The LDAP option is to provide a platform for the user that is using LDAP protocol service to able to use this Sync feature.

AD Sync can only supports customers configured with OpenLDAP in the most common setting.

CAPACITY

AVAILABILITY IP*edge* systems R1.2 and later.

RESTRICTION

- Active Directory (AD) sync tool won't allow users to change AD passwords. If password is expired, users must use Microsoft Windows or Microsoft Outlook to change their passwords.
- AD Sync tool is not using encrypted LDAP with SSL.
- AD Sync tool does not allow Admin to provide multiple values for Multiple Server Key when synchronizing users from multiple OUs of a domain.

HARDWARE No additional hardware is necessary for this feature.

FEATURE INTERACTION

IP*edge* License control: Ensure that there are End-Point and voice mail mailbox licenses available when creating SIP and IPT stations.