TIP/ix Support for LDAP

TIP/ws Direct Connect

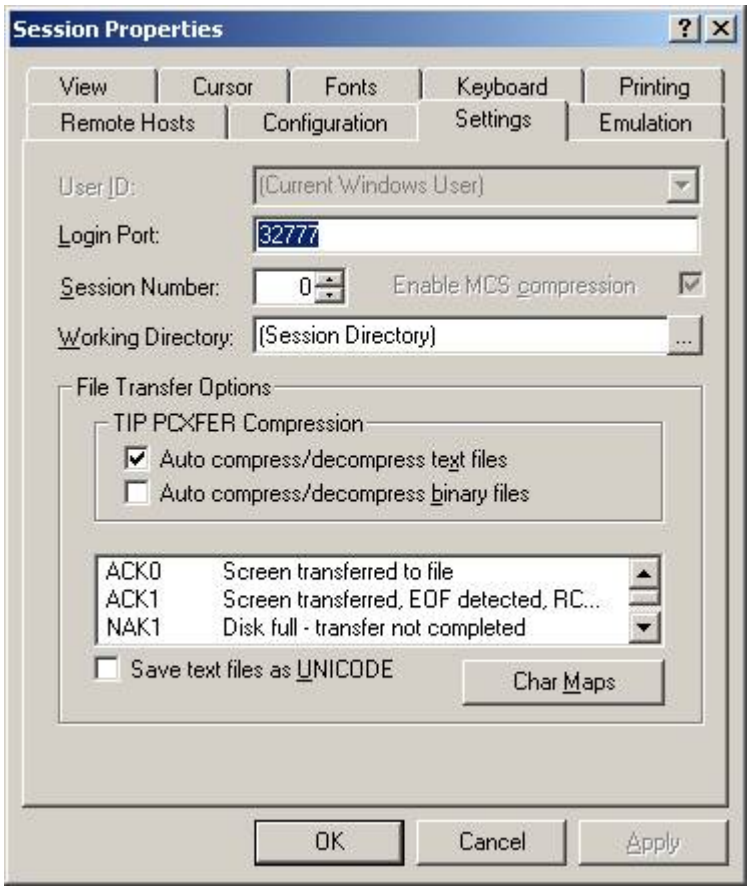
To have TIP/ix support TIP/ws Direct connect, add the following parameter to the `tipix.conf` file.

```
PARAM TIPWS=port#
```

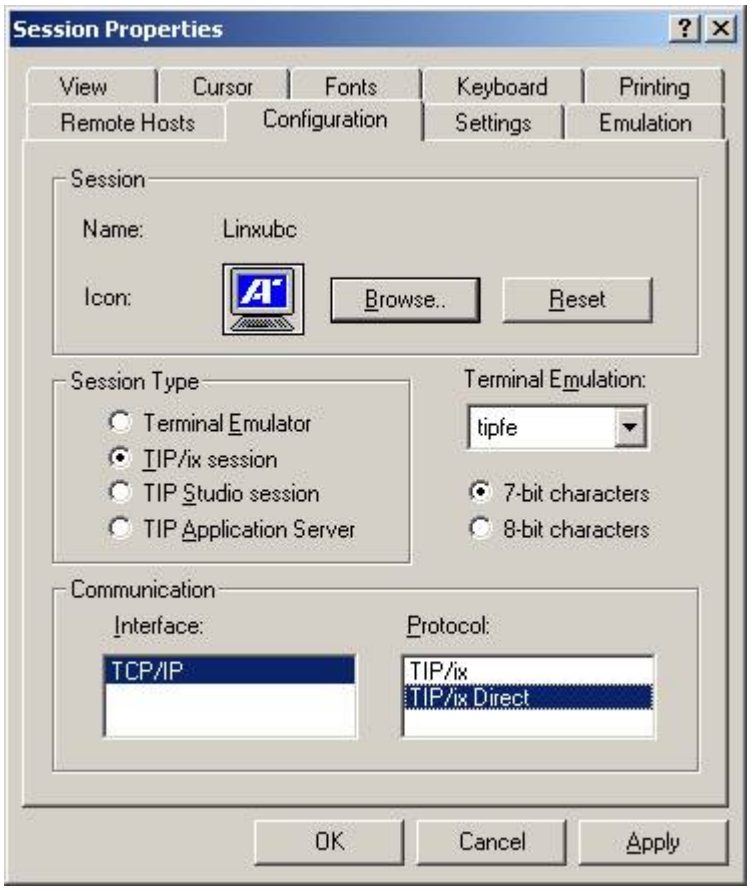
The port # is a TCP/IP port which is not used for anything else. You must also define the same port number to TIP/ws when you request the TIP/is Direct session protocol.

TIP/ws (Work Station) has been enhanced (Build 1423 or later) to optionally connect directly to TIP/ix, rather than having the user first log into Unix and then run the `tipix` user interface shell. This style of TIP/ws session is defined as follows:

The port number which TIP/ws is to use to connect to TIP/ix is defined under session properties on the settings tab. (This must match the value given to TIPWS in tipix.conf.)



In the session properties there is an option on the configuration tab o select TIP/ix Direct connect.



TIP/ix INT1 connection support

To have TIP/ix support the UTS INT1 protocol, add the following parameter to the `tipix.conf` file.

```
PARAM TIPINT1=YES
```

This will default to listen on port 256 for connections. If some other TCP/IP port is to be used then declare TIPINT1=port#.

If the INT1 terminal sessions are required to login, then add the extra parameter LOGIN. For example:

```
PARAM TIPINT1=LOGIN
```

If LOGON is required, then a UTS style screen is displayed for the end user to key in their user-id, password, and domain name (if needed).

You may also request TIP/ix user interface shell logging as follows:

```
PARAM TIPINT1=LOGIN,-aMl
```

With LOGIN requested, the user is presented with a screen format (TF$LGN0A) for them to enter their user-id and password. You may updated this screen format locally if you want different heading text or if you want to accept a longer password for Unix or Ldap authenication. The User-id must be no longer than 8 characters.

If you want to the user to be asked to logon in a command line style, then instead of the value LOGON, use DEMAND. For example:

```
PARAM TIPINT1=DEMAND
```

If you want TIP/ix to listen on more than one port, specify all port numbers (to a maximum of 3 different ports) that you want TIP/ix to accept connections on. For example:

```
PARAM TIPINT1=256,102,LOGIN
```

TIP/ix Configuration

In the `$TIPROOT/conf/tipix.conf` file there is a new parameter which indicates what method of authenticating users should be used for users who connect directly to TIP/ix using either TIP/ws or INT1.

PARAM LOGIN=UNIX	Indicates to use the Unix password
PARAM LOGIN=LDAP	Indicates to use LDAP for user authentication

The default is that the TIP/ix user security records managed by the `smuser` utility will be used for end user authentication.

TIP/ix LDAP configuration

For `LOGIN=LDAP`, there will be a configuration file called `$TIPROOT/conf/ldap.conf`. This `ldap.conf` file is initially created by the `tipldap` utility. This utility has the following parameters:

-i	Do the initial create of `ldap.conf`
-h	Define the LDAP server host(s)
-b	Define the LDAP Base Distinguished name for User searches
-s	Define the Admin User Secret password for searches. Optional
-P	Define the LDAP port to connect to; Default 389

For example:

```
tipldap –i –h sneezy:389 –b dc=inglenet,dc=com –s secret
```

The `tipldap` command creates `ldap.conf` and writes important information to it. Some of this information is encrypted for security reasons, so it is only visible to the

person who does the initial setup. The rest of the `ldap.conf` file has keywords which define the LDAP attribute name which is used to provide information to TIP/ix.

Keyword	LDAP Name	Max values	Type	Description
ACCOUNT	depIndex	1	9	The users account number. This will be used for the SAM 'department index value'.
BASEDN				Base distinguished name for searches
GROUPFILTER				Template string used as a filter for the group search
GROUPS	tipGroups	12	X	List of (max 8 character long) group names for transaction groups.
HOME	homeDirectory	1	X	Unix directory which is user's home location. If not given the default is $TIPROOT/tmpwrk/<uid>
LANGUAGE	tipLanguage	1	X	The 1 byte TIP/ix language code to be used for this user. If not given the default is the TIP/ix system language.
LOCATION	department	1	X	The department/location of this user. This will be used for the SAM 'department name'.
LOGIN				Default login distinguished name template string.
LOGINFILTER				LDAP Search Filter template string. Default is "uid=%U"
LOGINGROUPS				Define the attribute name that hold the TIP/ix group name. If this is defined as "dn", then the distinguished name(s) returned from the search are used
LOGINGROUPSEARCH				Base distinguished name for searching for the users

Keyword	LDAP Name	Max values	Type	Description
				group names
MAXUSER	maxUsers	1	9	Maximum number of users with this name that may be logged on at once. Default is unlimited.
NAME	cn	1	X	User common name
PASSWORD	userPassword	1	X	User password
SECURITY	tipSecurity	1	9	TIP/ix user security level 1 to 255. 1 is high, 255 is very low.
UNIXGID	gidNumber	1	9	The Unix group Id value for this user. If not given the default is the TIP/ix admin user group id.
UNIXUID	uidNumber	1	9	The Unix user id value for this user. If not given the default is the TIP/ix admin user id.
USER	uid	1	X	User identifier name. This will be truncated to 8 characters and used as the TIP/ix User name.

If the default LDAP attribute names do not match your LDAP server, then simply edit `ldap.conf` with any text editor and put in the correct values.

Some of the above keywords have a value which is a template string. This means that the template is parsed and some parts get replaced by other values.

%U is replaced by the User id

%D is replaced by the Users distinguished name

The keyword LOGIN is used to define a template used to search for the user's distinguished name string. For example:

```
LOGIN='uid=%U,ou=EXT,o=wgkk'
```

The **%U** is replaced by the user name supplied and the resulting string is passed to LDAP to search the BASEDN. The distinguished name which is returned is then available for replaced in other templates as %D. The distinguished name is also used along with the password to authenticate the user.

With TIP/ix the end user must supply the user-id and password. Optionally, a 'domain' name may be given. TIP/ix will search the `ldap.conf` for the domain name as a

keyword and then use its value for authenticating LDAP. If the domain name is not supplied or not found in ldap.conf then the LOGIN string is used. For example

```
ZULU='uid=%U,ou=users,dc=kup,dc=com'
TANGO='uid=%U,ou=users,dc=ibm,dc=com'
```

Then if the end user supplies TANGO as the domain name, the matched string is used for connecting to LDAP.

A sample `ldap.conf` file follows:

```
# Encrypted information for connecting to LDAP
HOST='m5#YJK:fT2}Gk6!}P'
PORT=389
BASEDN='jj3%5$OZ~c8HffpT&}'
ADMIN='Fbf<kwo7&~D~~zqc=i`}%M)((<Zem'
PWD='9nbw{~'
# TIP/ix Data Name = LDAP attribute name
LOGIN='uid=%U,ou=EXT,o=wgkk'
LOGINFILTER=”uid=%U”
USER='uid'
GROUPS='tipgrps'
NAME='cn'
HOME='homeDirectory'
PASSWORD='userPassword'
UNIXUID='uidNumber'
UNIXGID='gidNumber'

LOGINGROUPSEARCH="o=wgkk"
LOGINGROUPS=dn
GROUPFILTER="(&(objectClass=groupOfNames)(member=%D)(CN=$T_*))"
```

If the User Group membership is not part of the User’s attributes but needs to be read by a secondary LDAP search, then the LDAP search template is defined by the keyword LOGINGROUPSEARCH and the LDAP attribute to be returned is defined with LOGINGROUPS. For example:

```
LOGINGROUPSEARCH='uid=%U,ou=groups,dc=company,dc=com'
LOGINGROUPS=”groups”
```

Likewise, if a domain name is given and you need to have a separate group search for each domain they would be defined as follows:

```
ZULUGROUPSEARCH='uid=%U,ou=groups,dc=kup,dc=com'
ZULUGROUPS=”groupids”
TANGOGROUPSEARCH='uid=%U,ou=groups,dc=ibm,dc=com'
TANGOGROUPS=”groupnames”
```

LDAP Authentication Steps

The steps taken for authenticating the user and returning the information needed for TIP/ix are as follows:

1. Do an ldap search of BASEDN using the LOGINFILTER (merged with the User's id). This returned the User's distinguished name (DN).
2. Use the user's DN and given password to do an ldap bind. If this fails an error condition exists and the user is not allowed access to TIP/ix. They may retry.
3. An ldap search of the user DN is done to retrieve that various TIP/ix related attributes.
4. If LOGINGROUPSEARCH was specified, then an ldap search of that is done using the GROUPFILTER value.