



AN-288

Using Active Directory in Protege GX

Application Note



The specifications and descriptions of products and services contained in this document were correct at the time of printing. Integrated Control Technology Limited reserves the right to change specifications or withdraw products without notice. No part of this document may be reproduced, photocopied, or transmitted in any form or by any means (electronic or mechanical), for any purpose, without the express written permission of Integrated Control Technology Limited. Designed and manufactured by Integrated Control Technology Limited, Protege® and the Protege® Logo are registered trademarks of Integrated Control Technology Limited. All other brand or product names are trademarks or registered trademarks of their respective holders.

Copyright © Integrated Control Technology Limited 2003-2025. All rights reserved.

Last Published: 25-Sep-25 9:57 AM

Contents

Introduction	4
What is Active Directory?	4
Active Directory and Protege GX	5
Key Advantages	5
Active Directory for Operator Management	5
Active Directory User Integration	6
Data Sync Active Directory User Integration	7
Licensing	7
Active Directory Operator Integration	8
Prerequisites	8
Setting Up Windows Authentication	8
Enabling Windows Authentication Only	9
Enabling TLS 1.2 and Windows Authentication	9
Setting Up Operators	10
Logging In with Windows Authentication	10
Active Directory User Integration	11
Prerequisites	11
Active Directory User Import Settings	11
Data Sync Active Directory User Integration	12
Prerequisites	12
Data Sync Integration	12
PowerShell Script Sample	14

Introduction

Organizations from almost all sectors – IT, manufacturing, healthcare, and finance to name just a few – use Microsoft Active Directory services to provide centralized management of their servers, workstations and users. This application note describes the Protege GX integration with Active Directory and gives instructions for its configuration.

What is Active Directory?

Active Directory (AD) is a Microsoft Windows directory service that allows IT administrators to manage users, applications, data, and various other aspects of their organization's network. It also helps organizations maintain a central administration over all the activities carried out in their networks.

User accounts, computer accounts, groups, and all related credential information are stored in Active Directory.

Organizations primarily use AD to perform authentication and authorization. The Domain Service domain controller authenticates and authorizes all users and computers in a network, assigning and enforcing security policies for all computers.

AD is contacted before a user is granted access to a resource or service. When a user logs into a computer that is part of a Windows domain, Active Directory checks the submitted password. Once the authenticity of the user is verified, AD helps to determine whether the user is authorized to use that particular resource or service. If the user checks out on both counts, access is granted.

Active Directory and Protege GX

Protege GX's Active Directory integrations provide synchronization and authentication for Active Directory users, enabling organizations to leverage the user management and security policies that AD provides.

For our purposes, the important aspects of AD are:

1. Active Directory stores all Windows user logons, passwords and access permissions.
2. Active Directory uses those credentials to control access to computers and programs.

Because AD stores user information, we can use it as a synchronized source of users for Protege GX. And because it controls access to programs, we can use it to control operator access to Protege GX.

Key Advantages

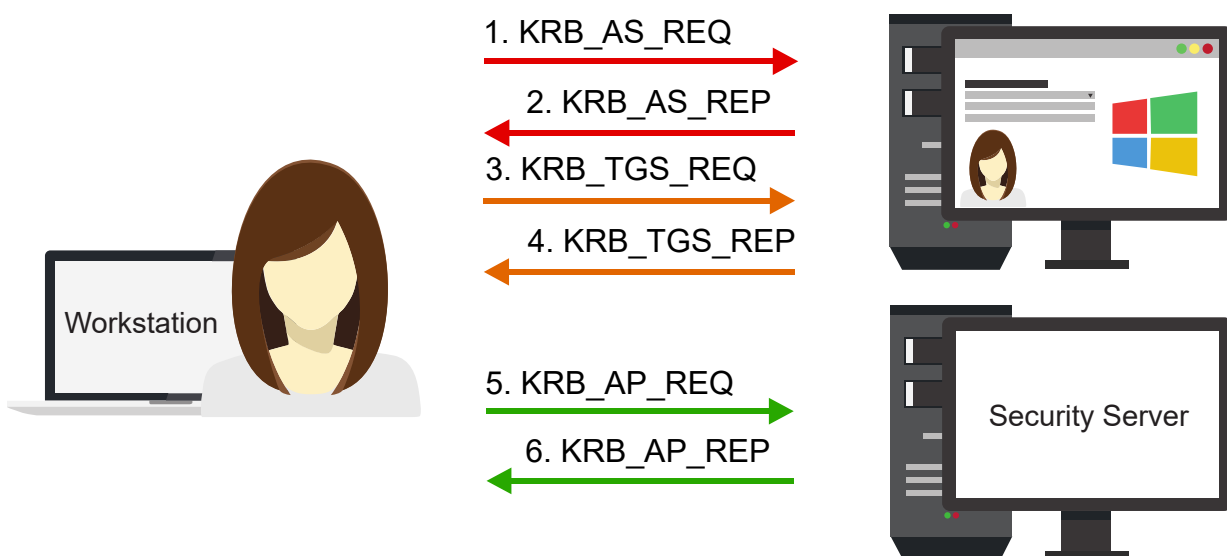
- Reduces administration and maintenance workload.
- Offers highly secure access through the usage of AD security policies.
- Provides centralized authentication while simplifying operator logon with single sign-on.
- Automatically creates and synchronizes Protege GX user accounts based on Active Directory users and groups.

Active Directory for Operator Management

Active Directory integration enables operators to log in to Protege GX automatically using their Windows credentials, providing centralized authentication and the convenience of single sign-on. Operators have one less password to remember, yet receive all the same password restrictions and security policies for that password as provided by Active Directory.

Active Directory details are configured under each operator record, and once defined the operator can select the option to use Windows Authentication. Protege GX then uses the operator's Windows network domain and user name automatically as authentication.

How it Works



When an operator attempts to log in using their Windows credential, the Kerberos network authentication service specifies six messages (five mandatory and one optional), grouped into three pairs of sub-protocols:

The Authentication Service (AS) exchange takes place at logon, and is concerned with giving clients the right to request tickets to access resources.

1. The client sends a **KRB_AS_REQ** authentication request to the KDC (Key Distribution Centre).
2. If approved, the KDC will generate a ticket granting ticket (TGT) which is returned to the client as part of the **KRB_AS_REP** authentication reply.

The Ticket Granting Service (TGS) exchange commences when the client requires access to a resource.

3. The client sends a **KRB_TGS_REQ** service ticket (ST) request to the KDC with the name of the service to which access is required.
4. The KDC will validate the authentication token within the TGT and, if permitted, return a service ticket which is valid for the requested service as part of the **KRB_TGS_REP** reply.

At this stage the client is not authenticated. The service ticket is only valid between the user and the service, but provides mutual authentication.

The Client/Server (AP) exchange is the authentication protocol, where the client presents a service ticket and an authenticator to a service to establish an authenticated communication session with the service.

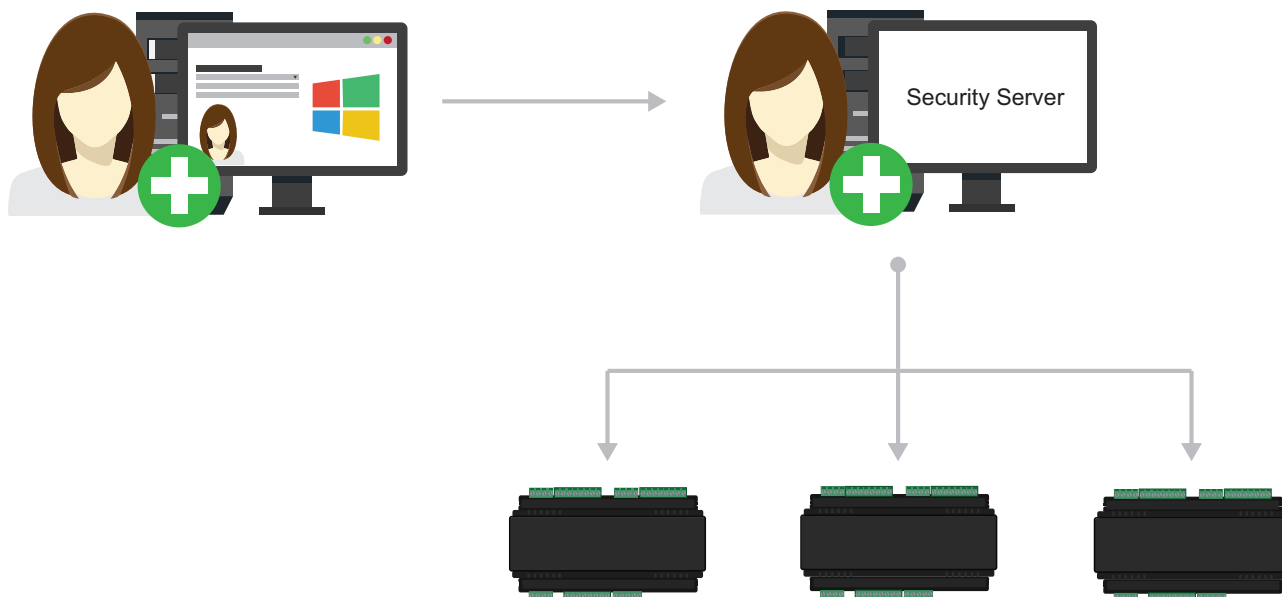
5. Only after the client has sent a **KRB_AP_REQ** request to the service server, and there is mutual authentication, will the client be authenticated and allowed access to the requested resource.
6. The service server may or may not send a **KRB_AP_REP** reply.

At all stages, only the KDC can read the TGT and only the service can read the ST.

Active Directory User Integration

Active Directory integration enables you to leverage the user data already contained in your Microsoft Windows Domain to create and maintain Protege GX users.

This integration works by obtaining a list of users based on the defined Active Directory security group, importing the user names and current AD status (active or disabled), then synchronizing them as frequently as desired.



New users are automatically added to Protege GX as they are added to Active Directory without the need for administrators to intervene.

Synchronization ensures that if there are any changes made to the Active Directory profile, then the Protege GX user record is updated, and if a user is disabled or deleted within Active Directory, their Protege GX user account is also disabled.

Data Sync Active Directory User Integration

Active Directory integration using Data Sync provides a more sophisticated level of user integration, with fully customizable access to the user data already contained in your Microsoft Windows Domain.

This feature can be used to import and update access levels, departments, car registration, even sporting teams. Any user data in Active Directory can be mapped to any field in Protege GX, existing or custom, to create and maintain Protege GX users with selected AD properties.

The integration works by running a configured ICT Data Sync Service import, with customized user data synchronized from Active Directory as often as required. User data is retrieved from AD and exported to a CSV file. The ICT Data Sync Service then reads the data in the CSV file and uses the Protege GX SOAP Service to import the records to Protege GX.

Licensing

The Active Directory Operator and User integrations are all optional licensed features that add functionality to an existing Protege GX system. Each requires a specific license, which is applied to the server.

Each integration option is licensed separately.

- PRT-GX-AD-OPR : Active Directory Operator Integration License.
- PRT-GX-AD-USR: Active Directory User Integration License.
- PRT-GX-DB-SYNC: Data Sync License for Data Sync User Integration.

Active Directory Operator Integration

Integrating Protege GX with Active Directory allows operators to log in to Protege GX using Windows Authentication. If the operator is logged in to the Windows domain, they can automatically log in to Protege GX without entering their username and password.

It is also possible to use Windows Authentication to log in to the Protege GX Web Client. After completing the instructions in this document, refer to [Application Note 299: Using Windows Authentication with the Protege GX Web Client](#).

Prerequisites

Licensing

Active Directory operator integration is an optional licensed feature. Purchase the following license from ICT:

- PRT-GX-AD-OPR : Active Directory Operator Integration License.

Windows Domain

Ensure that Protege GX server and client are set up on the Windows domain, as follows:

- The Protege GX Data Service machine (i.e. the Protege GX server) must be joined to the Windows domain.
- The Protege GX Data Service must run under the NT AUTHORITY\SYSTEM account (default). It cannot be run under a domain account or a local machine account.
- In order to log in with Windows Authentication, client workstations must be on the same Windows domain as the Protege GX Data Service. Clients outside the domain can still log in with a username and password.

Server Name and IP Address

Operators need to specify which server they are connecting to as they log in to Protege GX. When Windows Authentication is enabled, they must enter the server details as follows:

- **On the server:** The operator must specify the **computer name** of the server. They can no longer leave the field blank or enter localhost.
- **On clients within the domain:** The operator must specify the **computer name** of the server.

It is possible to configure the Windows domain to accept the server's IP address as a hostname. If this is required, refer to the [Microsoft documentation](#) and consult the site's IT team.

- **On clients outside the domain:** The operator must specify the **Fully Qualified Domain Name (FQDN)** of the server.

Setting Up Windows Authentication

When you install Protege GX, you must choose whether the installation will use TLS 1.2 or Windows Authentication. Both methods provide encrypted communications, but have different configuration and requirements.

If you wish to allow operators to log in with Windows Authentication, there are two options:

- **Windows Authentication only:** Suitable for most sites. Follow the instructions in [Enabling Windows Authentication Only](#) below.
- **TLS 1.2 and Windows Authentication:** Some sites require TLS 1.2 as well as Windows Authentication for compliance reasons. Using TLS 1.2 with a custom certificate can also make it easier for clients outside the firewall to connect to the Protege GX server. If both protocols are needed, follow the instructions in [Enabling TLS 1.2 and Windows Authentication](#) below.

In both cases, we also recommend that you disable the legacy NTLM protocol, as instructed below.

Enabling Windows Authentication Only

To enable Windows Authentication, you must select the **Enable Windows Authentication on Data Service / Client Communications** setting when you install Protege GX. This setting must be enabled on the Protege GX server and all client workstations.

Disabling NTLM

We recommend that you disable the legacy NTLM protocol to improve your communication security. You must use a Windows group policy to disable this protocol. Discuss with the site's IT team.

Enabling TLS 1.2 and Windows Authentication

Configuring TLS 1.2

If you wish to implement both TLS 1.2 and Windows Authentication, you must set up TLS 1.2 **first**.

Follow the instructions in the Protege GX Installation Manual or Application Note 277: Configuring Protege GX to use TLS 1.2 to install Protege GX and set up TLS 1.2. In particular, complete the following tasks:

- When you install the Protege GX server and clients, select the **Enable TLS 1.2 Authentication on Data Server / Client and SQL Server Communications** setting.
- Enable force encryption, TCP/IP and the IIS management console.
- If required, install a custom TLS 1.2 certificate from a trusted source and enable certificate validation. This enables clients to connect from outside the firewall.

Before you continue, validate that TLS 1.2 is working correctly by checking that remote clients can log in to the server.

Enabling Windows Authentication on the Server

Once TLS 1.2 is enabled, you can enable Windows Authentication on the Protege GX server.

1. In a File Explorer, navigate to the Protege GX installation directory. By default, this is:
C:\Program Files (x86)\Integrated Control Technology\Protege GX

2. Open **GXSV.exe.config**.

Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

3. Locate the following section in the XML:
/configuration/system.serviceModel/bindings/netTcpBinding/binding[@name="Binding1"]/security

4. **Replace** the existing security node with the code below:

```
<security mode="TransportWithMessageCredential">
  <transport clientCredentialType="None"
  protectionLevel="EncryptAndSign" sslProtocols="Tls12"/>
  <message clientCredentialType="Windows"/>
</security>
```

5. **Save** the config file.

6. Restart the **Protege GX Data Service**.

Enabling Windows Authentication on the Clients

You must also edit the Protege GX client config file on every workstation that will be used to log in to the server. This includes the client config file on the server machine, as well as any other workstations with the client installed.

At the same time, we recommend that you disable NTLM on the client installations to improve your communications security.

1. In a File Explorer, navigate to the Protege GX installation directory. By default, this is:
C:\Program Files (x86)\Integrated Control Technology\Protege GX

2. Open **GXPI.exe.config**.

Files in this directory require administrator permissions to edit. You may need to open the file as an administrator using an application like Notepad++, or make a copy in a different directory to edit and replace the original.

3. Locate the following section in the XML:

```
/configuration/system.serviceModel/behaviors/endpointBehaviors/behavior  
[@name="md0"]/clientCredentials/
```

4. **Add** the configuration line below as a child of the **<ClientCredentials>** element:

```
<windows allowNtlm="false"/>
```

5. Locate the following section in the XML:

```
/configuration/system.serviceModel/bindings/netTcpBinding/binding[@name="Binding1"]/security
```

6. **Replace** the existing security node with the code below:

```
<security mode="TransportWithMessageCredential">  
  <transport clientCredentialType="None"  
  protectionLevel="EncryptAndSign" sslProtocols="Tls12"/>  
  <message clientCredentialType="Windows"/>  
</security>
```

7. **Save** the config file.

Setting Up Operators

You can now enable Windows Authentication for operators by mapping them to Active Directory users.

1. To enable Windows Authentication for an operator, navigate to **Global | Operators**.
2. In the Configuration settings, enable **Use Windows Authentication**.
3. Click the ellipsis [...] beside the **Username** to search for the Active Directory users record for the operator.
4. Enter the operator's **Username** or name and click **Search**.
5. Select the **Domain** from the drop-down list if required.
6. Select the operator's user record from the list of AD Usernames displayed below, then click **OK**.
7. The operator's AD user credentials should now be displayed in the Username.
8. Once the operator's AD credentials have been verified, click **Save**.

Logging In with Windows Authentication

When your operator record has been mapped to an Active Directory user, you can log in to Protege GX without entering a username or password.

1. Start Protege GX.
2. When the login window is displayed, select the **Use Windows Authentication** option.
3. Specify the Protege GX **Server** you are connecting to. This must be the **computer name** if you are connecting from within the domain, or the **Fully Qualified Domain Name (FQDN)** if you are connecting from outside the domain.
4. Click **Log in**. You will be logged in with your Windows user credential, as long as it is valid.

Active Directory User Integration

The Active Directory user integration enables the import of Active Directory users into the Protege GX system based on the active directory group that has been selected.

Prerequisites

Active Directory user integration is an optional licensed feature that requires a Protege GX Active Directory User Integration license applied to the server.

- PRT-GX-AD-USR: Active Directory User Integration License.

Active Directory User Import Settings

Enabling the Active Directory user integration requires configuration of the Active Directory user import settings. This allows Protege GX to import and synchronize Active Directory user records with Protege GX users. Navigate to **Global | Sites | Active Directory**.

- **Import users from Active Directory:** Select this option to import user details from Active Directory to the Protege GX database.
- **Active Directory domain:** Defines the Windows Active Directory domain being used.
- **Windows group:** The Windows group containing the users to import.

Only one selected Windows security group can be synchronized with this integration.

- **Synchronization period (minutes):** Defines the frequency of synchronizing users with Active Directory.
- **Disable users if AD users are disabled:** Disables Protege GX user access if the Active Directory account is disabled.
- **Disable users if AD users are deleted:** Disables Protege GX user access if the Active Directory account is deleted.

Data Sync Active Directory User Integration

The Data Sync Active Directory user integration provides an advanced customized import and synchronization of Active Directory users into the Protege GX system, including multiple AD groups and custom user criteria.

Any field that exists in Active Directory can be mapped to any field that exists in Protege GX. Even if the field is not automatically included in Protege GX it can be added as a custom field, bringing great power to utilize AD user data.

PowerShell Script

A customized Windows PowerShell script will be required to retrieve the necessary Active Directory user data and export it to a suitably configured CSV file. This is a complex script requiring knowledge of Windows PowerShell and your network domain and security configuration.

The attached sample (see page 14) provides a basic indication of the type of process and fields required, but there is potential for far more complex and useful user criteria to be synchronized. Please consult your IT professional for assistance with this process.

The PowerShell script should always contain at least a Unique Identifier, First Name, Last Name, and a Status field to identify whether users are enabled or disabled.

Prerequisites

Data Sync Active Directory user integration is an optional licensed feature that requires a Protege GX Data Sync license applied to the server, along with specific software and licensing requirements.

Software Requirements

All software must be installed and operational.

Software	Version
Protege GX	4.2.214 or higher
Protege GX SOAP Integration Service	1.5.0.19 or higher
ICT Data Sync Service	2.0.0.0 or higher

Licensing

License	Order Code	Notes
ICT Data Sync Service License	PRT-GX-DB-SYNC	1 per server
Protege GX Client Connection License	PRT-GX-CLNT	If using a version of the ICT Data Sync Service prior to 2.0.6.3 and a version of the Protege GX SOAP Service prior to 1.5.0.27, a Protege GX client connection must be available for use by the service.

Data Sync Integration

The following steps are required to program Active Directory user synchronization using the ICT Data Sync Service.

- It is assumed the ICT Data Sync Service is installed and configured, with the appropriate license applied.
- It is assumed Protege GX SOAP Service is installed and configured, with the appropriate license applied.

- It is assumed that the customized PowerShell script has been supplied (see next page).

Programming

The main programming steps are:

- Export Active Directory users to a CSV file, using a customized Windows PowerShell script
- Import Active Directory users from the CSV file into Protege GX, using the data sync service

Export Active Directory Users to a CSV File

1. Right click the Windows PowerShell script file and **Run with PowerShell**.
This process may take seconds or minutes, depending on the file size.
2. Locate the CSV file created by the above process. It is recommended to check the file to ensure that the export has completed as expected and the data is correct before continuing.

Import Active Directory Users from the CSV file into Protege GX

1. Open the **Data Sync Service Configuration Tool**.
2. Select the **Target System**. This would typically be Protege GX but will depend on your system configuration.
3. Enter the **SOAP Server Address**. This is the server where your Protege GX SOAP Service is installed.
4. Enter the **Username** and **Password** for this Data Sync synchronization.

A unique **Operator** should be created specifically for this process to enable targeted event reporting.

5. Select the **Site** to synchronize.
6. Under **Data Mapping** select the **Record to Sync**. This is the Protege GX database table that you want to map and import AD user records into. This would typically be the `Users` table but it is possible to create more customized integrations.
7. Specify the **Data Source** to be imported by selecting the **File Directory** (folder location) and **Import File**.
8. The **Start Import At Row** setting will usually need to be changed to **Row 2**, as Row 1 typically contains the file headers and is not user data to be imported.
9. In the mapping window below, map each **Source Column** from the AD users CSV file to the appropriate **Target Field** in the Protege GX **Record to Sync**.
The unique identifier must be mapped to a **Unique Field**. This would generally be a custom field (`CustomField1` is recommended).
10. Any fields that contain true or false values, such as a Disabled User field, will typically be exported to the CSV file in ALL CAPS. These must be converted to lower case.
 - Click the **Advanced** button in the row of the required Target Field.
 - In the **Conversion** table, enter the Original Value of TRUE, with a Resulting Value of true.
 - In the second row, enter the Original Value of FALSE, with a Resulting Value of false.
 - Click **OK** to save.

11. **Save** the configuration.
12. Then **Start** the data sync import.
13. Under **Sync Options** set the **Resynchronize Every** setting to the required number of minutes or hours for the synchronize process to run and update user records.
14. Click **Save** to update the configuration

Imported results and user details can be viewed in Protege GX under **Users | Users**.

PowerShell Script Sample

```
Import-Module ActiveDirectory
# CSV path for exported users
$CSVpath = "C:\DataSync\ADUsers.csv"

$users = Get-ADGroup -Server "svr1.yourdomain.local" -Filter * -SearchBase
"OU=Building Security,OU=Security Groups,OU=Users,DC=Domain Users" | Get-
ADGroupMember | Sort | Get-Unique | Get-ADUser

$myData = $users | Select-Object -Property @{Name="UniqueID";Expression={ -
join ($_.ObjectGUID.ToByteArray() | foreach { $ofs="" } { "{0:X2}" -f $_})}},
@{Name="FirstName";Expression={$_.GivenName}},
@{Name="LastName";Expression={$_.Surname}},
@{Name="FullName";Expression={$_.name}},
@{Name="DisableUser";Expression={ !($_.Enabled)}}

$myData | Export-csv -path $CSVpath -notype

$a = "<SOF>"
$b = Get-Content "C:\DataSync\ADUsers.csv" | Where { $_ -notmatch "UniqueID" }
$b = $b -replace ";\\s", ";"
$c = "<EOF>"

Set-Content "C:\DataSync\ADResults.csv" $a, $b, $c
Move-Item "C:\DataSync\ADResults.csv" "C:\DataSync\Output\ADResults.csv" -
force
```

Designers & manufacturers of integrated electronic access control, security and automation products.
Designed & manufactured by Integrated Control Technology Ltd.
Copyright © Integrated Control Technology Limited 2003-2025. All rights reserved.

Disclaimer: Whilst every effort has been made to ensure accuracy in the representation of this product, neither Integrated Control Technology Ltd nor its employees shall be liable under any circumstances to any party in respect of decisions or actions they may make as a result of using this information. In accordance with the ICT policy of enhanced development, design and specifications are subject to change without notice.