

# Instinct - How to Switch to Active Directory Security V5.3 and Above

Use this how-to guide to Setup Instinct Active Directory Security.

Instinct can be used via Instinct Security or Active Directory Security. By Using Active Directory Security, you gain the following benefits:

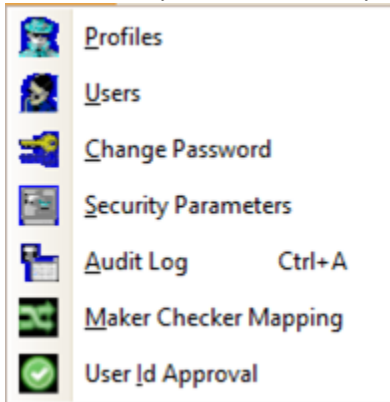
1. Easier for users as there is no additional password for them to remember.
2. Assurance that Instinct will meet your existing security requirements

Before you switch Instinct to Active Directory Security you need to do the following:

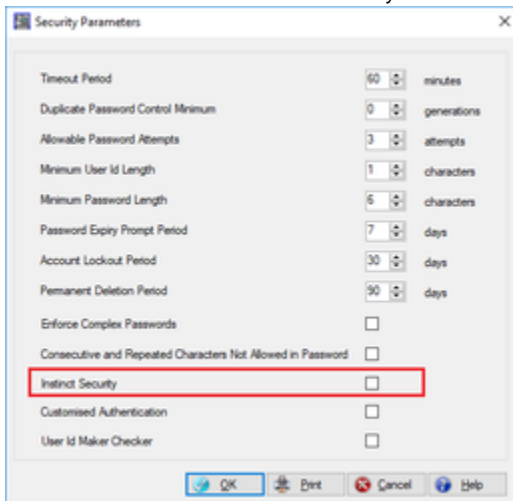
1. In Active Directory create the Security Groups required.
2. Add the Active Directory Users to the required Security Group.
3. In Security > Profiles menu define the access you desired for each Security Group. The Profile Name must match the Active Directory Security Group Name exactly. For Example: if the Active Directory Group name is 'Instinct – Fraud Managers' then the Instinct Profile Name must be 'Instinct – Fraud Managers'.

Switching Instinct to Active Directory Security

1. From the Security menu select Security Parameters.



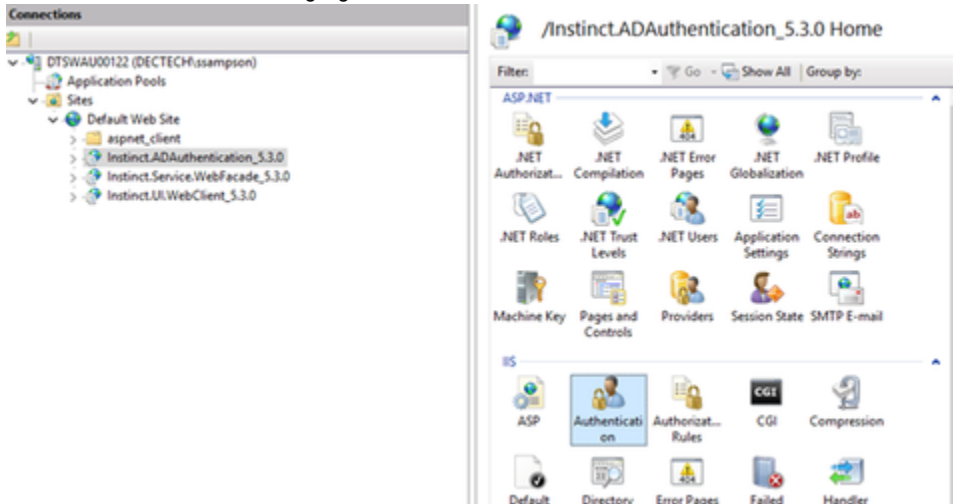
2. Remove the tick from the Instinct Security tick box.



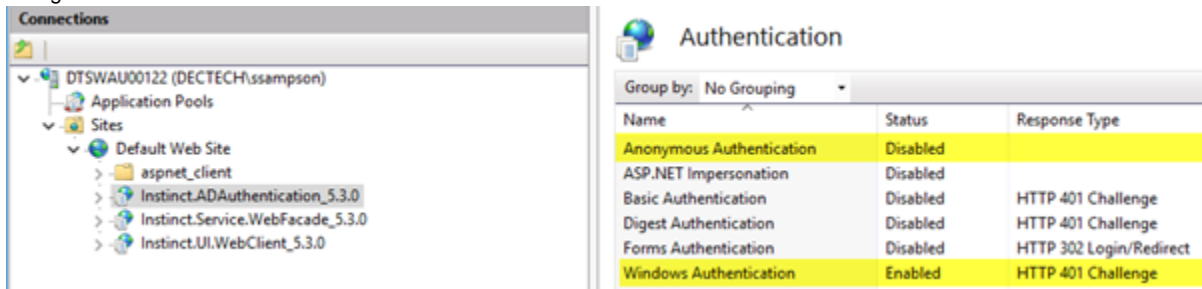
3. Select the OK Button

Enabling Windows Authentication for Instinct web Server

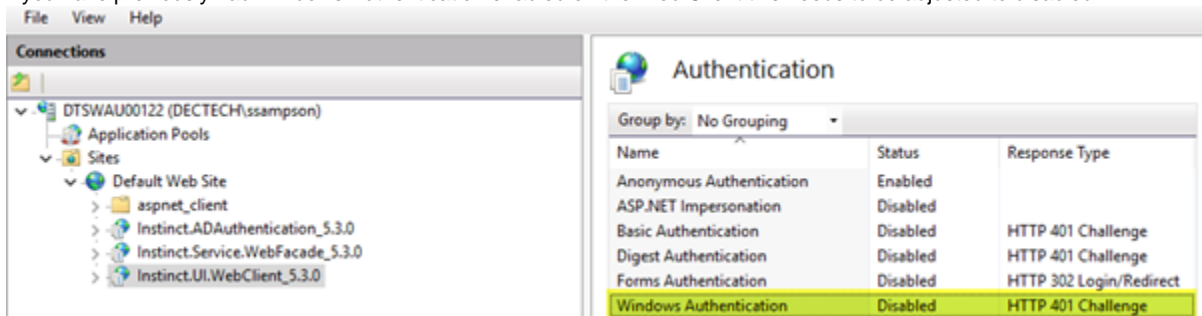
1. Select the Instinct web server highlight the AD authentication client and double-click the Authentication icon.



2. Right-click on the Windows Authentication option and change to Enabled. Right-click on the Anonymous Authentication option and change to Disabled.



3. If you have previously had Windows Authentication enabled on the Web Client this needs to be adjusted to disabled



4. Open Web Client Web config, Ensure that the Instinct.ADAuthentication Parameter point to the correct Instinct.ADAuthentication path.

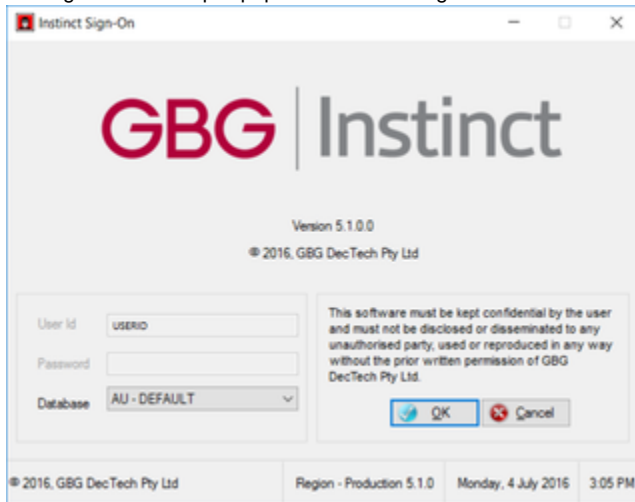
```
<appSettings>
  <!-- Please encrypt this appSettings block using the Installation utility provided with Instinct -->
  <add key="Security.TokenSecret" value="f80d9reukM_W5WkQIBH1QnJ9wAB-g0fshCRFwyo" />
  <add key="Security.SslEnabled" value="false" />
  <add key="Support.Telephone" value="(41) 1800 312 840 (Monday to Friday, 9:00 a.m. to 5:00 p.m. local business hours)" />
  <add key="Support.Email" value="customer.support@hugobc.com" />
  <add key="Client.Timeout" value="600" />
  <!-- Seconds -->
  <add key="Token.Timeout" value="180" />
  <!-- Minutes -->
  <add key="InputFile.Format" value="ASCII" />
  <add key="Security.Timeout" value="0.5,10,15" />
  <add key="Print.CsvWriter" value="1" />
  <add key="Instinct.BaseProduct" value="Instinct" />
  <add key="Instinct.DateDisplayFormatMoment" value="DD/MM/YYYY" />
  <add key="Instinct.DateDisplayFormatDotNet" value="dd/MM/yyyy" />
  <add key="Instinct.IsTime4hrsFormat" value="false" />
  <add key="Instinct.SSOUserKey" value="" />
  <add key="Instinct.SSOLogoutPage" value="" />
  <add key="Instinct.SSOLogoutPage" value="" />
  <add key="Instinct.ADAuthentication" value="https://localhost/Instinct/InstinctADAuthentication_080_5.3.3.4" />
  <add key="Instinct.BatchFileDelimiter" value="|" />
  <add key="Instinct.TempDirectory" value="C:\GBO\Instinct\WebClient\EXPORT" />
  <add key="Instinct.WriteLog" value="1" />
  <add key="Instinct.LogDirectory" value="C:\GBO\Instinct\WebClient\temp" />
  <add key="Instinct.DelimiterCharacter" value="|" />
  <!-- LDAP Customised Authentication -->
  <add key="LDAPServer" value="192.168.0.1:389" />
  <add key="LDAPUserDN" value="uid=admin,ou=people,dc=DECTECH,dc=COM" />
  <add key="LDAPPassword" value="Instinct" />
  <add key="LDAPUserSearchBase" value="ou=people,dc=DECTECH,dc=COM" />
  <add key="LDAPUserSearchFilter" value="(snp: (objectClass=DecTechPerson) (uid=#11111) (memberOf=InstinctGroup))" />
  <add key="LDAPCertificatePath" value="" />
  <add key="LDAPSSL" value="N" />
</appSettings>
```

5. If configured correctly, the Instinct web client will perform an authentication challenge at the login page. If the challenge is successful, the username will auto-populate, and the password will be bypassed. The authentication challenge will pass any domain profiles to Instinct to match for profile authorization.

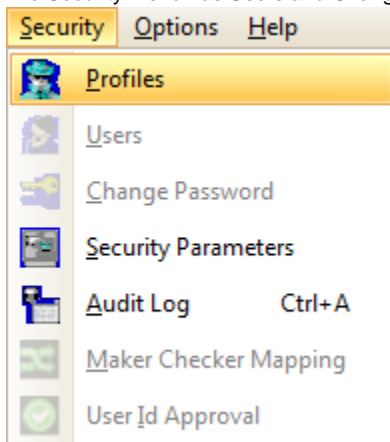
**Important:** Do not close the existing Instinct Session. If the switch to Active Directly Security is not successful, you will need the session open to change the security back. If you do close the session and you are unable to log back into Instinct the access can only be changed back via the Database. Contact GBG for assistance should this occur. Open a new session of the Instinct Client from the Desktop or the Programs Menu.

The following changes will have occurred:

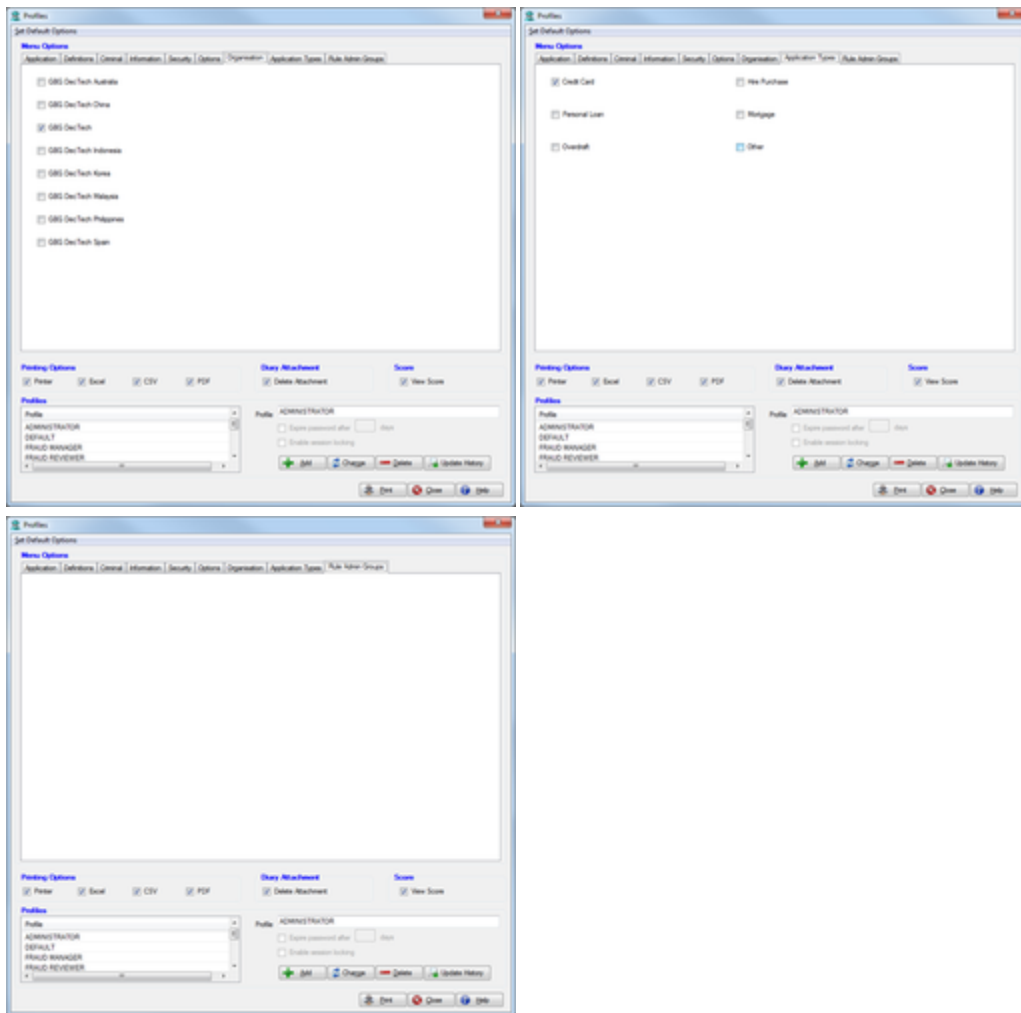
1. The login window is pre-populated with the logon of the local user and the Password field is disabled. Select the OK button to logon.



2. The Security menu has Users and Change Password disabled.



3. On the Security Parameters window none of the parameters apply as these are all controlled by Active Directory.
4. On the Profiles window there are three additional Tabs 'Organisation', 'Application Types' and 'Rule Admin Groups'. Previously the controls for these were on the Users window, as this is now disabled you need to update your Profiles to allow the appropriate access.



## Related articles

- [How to Switch to Active Directory Security V5.3 and Above](#)
- [How to configure directory from Instinct Batch and Online services](#)
- [Error Length of the data to decrypt is invalid](#)
- [How to Switch to Active Directory Security V5.2 and Below](#)