Security Considerations using Synthesys

Overview
Every call centre have their own considerations for security of data. This document describes how these measures might interact with the Synthesys system, and also describes some of the security features built in to Synthesys.
This document is not a replacement for a thorough understanding and implementation of industry best practices for security.

Synthesys Application Level Security

User Logon
Each user of Synthesys is given a username and password. The username is used in several ways in the Synthesys system for control and auditing. For added security, Synthesys logon can be integrated with Windows logon.

Auditing
Any action taken from within the Synthesys system, such as taking a call, designing a callflow, or taking an action in Synthesys, is logged against that username in the Synthesys database.

Application Control
Only privileged Synthesys users are allowed to access different parts of the system. This table outlines the different permissions available in the system.

Permission Name	Details
Design Scripts	Creation of call centre scripts.
Release Scripts	Distribution of scripts to the call centre agents.
Take Calls	Normally given to all call centre agents.
Manage Personnel	Create new users, modify permissions on personnel.
Outbound Manager	Change properties of outbound campaigns, create new outbound campaigns.
Manage Teams	Move agents between different teams, create teams.
Queue Calls	Queue calls for outbound dialling.

Teams
Synthesys also has the concept of teams. Agents can be placed in one or more teams. Likewise, campaigns can be put in teams. Agents may only take calls for a campaign if they share a team with that campaign.
Synthesys teams are chiefly used for organising outbound workload, and for providing a workflow element into Synthesys. However, they can also be used to restrict access to sensitive campaigns to selected users.

Windows Security and Synthesys

Synthesys workstations need to communicate with the Synthesys server. There are three communication channels used, all of which run over a normal Ethernet LAN or WAN running the TCP/IP protocol.

File Sharing
Synthesys workstations require access to the \\servername\synthesys share. There are two main reasons for this when taking calls. First, Synthesys automatically copies

new Synthesys binary files and scripts from the server when they are available. Secondly, when a call is complete, it is written to a pending directory on the server, from where it is inserted into the database by a Synthesys server component.
Recommendation : The security on the Synthesys share and the directories within it should be set up so that non-Synthesys users cannot see the share at all; normal users will have restricted access, and only administrators can access the whole Synthesys directory.

TCP/IP protocol
Synthesys Workstation communicates with components on the server, for example to retrieve lists of active calls on the system.
Recommendation : If deployed in a non-secure scenario, where hacking into the system might be a problem, then the Synthesys server should be protected from unauthorised TCP/IP connections using a firewall.

Database Access
Synthesys Workstation also reads from the Synthesys database. There are two supported configurations here. We usually recommend setting up a Synthesys user on the database. This has an encrypted password, so that only Synthesys applications can access the database. In this case, Synthesys application security protects data in the database.
Alternatively, Windows Trusted Connections can be used; in this case, normal SQL Server security measures can be used to protect tables. However, this can be time consuming to set up.
Recommendation : If Database Security is a concern, the simplest secure solution is to use an encrypted password with the trusted Synthesys user.

Workstation Security
If workstations are 'locked down', then Synthesys will still work fine. However, it is necessary to log on as a user with Administrator or Power User rights to install or upgrade Synthesys.

Data link security

Normally call centres work over a LAN, in which case the premises containing the LAN are expected to be secure.
If the LAN is not trusted, or Synthesys is to be over a WAN, then IP traffic snooping might be a risk. In this case, a VPN using a secure protocol (L2TP for example) would be a solution.
Recommendation : If confidential information is to be send over a WAN, then all traffic should be encrypted using a VPN.

Terminal Services / Citrix

In the light of some of the points above, a simpler solution when implementing over a WAN is to implement a Terminal Services (or Citrix) solution, which can also reduce bandwidth requirements. In this case, communication should still be secured by SSL or a VPN.

Synthesys.NET

Synthesys.NET is the version of Synthesys which allows scripts to be run over a web link. Data is transferred from the client to the server over HTTP or HTTPS secure protocols. HTTPS ships with all current browsers, and can be enabled on the server by installing an appropriate security certificate.

Recommendation : For capture of confidential information over the web, HTTPS protocol should be used. Additionally, all Microsoft security bulletins should be monitored, and patches applied as required.