

Case Study

Healthcare Trust reduces costs and management overheads with Celestix WSA remote access appliance and HOTPin tokenless two factor authentication



“In these days it’s hard to find a product that does what it says on the tin and the Celestix Network’s WSA IAG solution, with HOTPin does just this”

- Nick Rackham, Technical Programme Manager for Suffolk Support Services

Suffolk Mental Health Partnership NHS Trust operates from over 60 sites, with the Trust’s head office based at Clement’s Hospital, in Ipswich. Suffolk Mental Health Partnership NHS Trust provides a clinical service to all ages with learning disabilities, substance misuse and eating disorders.

Suffolk Mental Health Partnership NHS Trust has a dedicated team, Suffolk Support Services, which manages the infrastructure across 183 sites and for over 7600 IT users. Users are typically clinical and business users in nature and may be based at sites or working remotely, requiring access at any time of the day.

The organisation needs to provide access to a broad range of applications and resources to users with varying levels of authority. The challenge has been to provide granular, controlled and secure remote access whilst ensuring good value for money.

With help from Celestix Networks, Suffolk Support Services implemented two WSA6000 appliances running Microsoft Intelligent Application Gateway (IAG) 2007, a CLB4000 load balancer to provide an active/active configuration, and HOTPin, a tokenless two factor authentication solution using SMS and soft token technology.

The result of deploying this solution is more flexible yet controlled remote access, with fewer help desk calls, lower cost but greater security over centralised resources.

Situation

Until 2006 Suffolk Mental Health Partnership NHS Trust was using dial-up access with watchword tokens for remote workers. Dialling up was proving to be time consuming for end-users and for the ICT team.

The ICT team was experiencing high volumes of calls from frustrated employees having problems with their connection. In

addition, users were failing to remember to carry their tokens around with them and the tokens regularly needed to be replaced.

In response to the limitations and increased cost implications of extending this dial up solution Nick Rackham, Technical Programme Manager, identified a need for a more robust secure remote access solution to overcome the daily dial-up issues they were facing. Investigations with Connecting for Health (CfH) lead to the installation of a Cisco IPSEC solution with RSA tokens then issued to remote users.

Soon after deploying this solution it was realised that the solution could only be a short-term fix as the solution would not support the forever growing Trust. The Cisco and RSA solution was expensive and expanding the deployment would mean procuring additional hardware and more tokens.

The ICT team were faced with their original problem, more phone calls from frustrated remote employees, limitations of the solution, and extra cost to deliver increased usage.

To add to these issues, in 2009 flu pandemic became a national crisis which led to an increase in the number of temporary staff. This put an additional strain on an already stretched network.

Solution

By 2009 the increase in the number of remote users combined with increased help desk calls and a desire to publish a greater range of applications led the ICT team to investigate alternatives to the Cisco IPSEC solution.

Nick contacted CfH for guidance and they recommended Microsoft IAG 2007 to accommodate Suffolk’s new requirements.

Microsoft IAG was already in use at CfH and is recognised as a very relevant solution for organisations in the healthcare

“Far easier route to access systems and applications than ever before”

- Nick Rackham, Suffolk Support Services

“We needed to increase the amount of users, without the added expense required for additional hardware”

- Nick Rackham, Suffolk Support Services

“The user experience has been simplified and at the same time access to our data has never been more secure and helpdesk costs have reduced.”

- Nick Rackham, Suffolk Support Services

sector. Nick spoke with Celestix Networks and the recommendation was to deploy two Celestix WSA6000 units, with Celestix Load Balancer (CLB) to provide a stable platform for IAG 2007.

Celestix also provided an answer to the issue of physical tokens with their HOTPin solution which delivers one time passwords to remote users either through a soft token on the users' smart phone or laptop, or via SMS for users without a smart device.

IAG on the WSA6000 allows for browser based remote access to a broad range of applications regardless of type. As a result, Suffolk can now provide access to a wider list of resources including various Citrix based applications, SharePoint, OWA, RDP and intranet services.

In addition, Suffolk can now deliver tailored end user experiences dependent on the credentials of the user. Two portal trunks are configured to allow IT users a completely separate log in process to standard users.

By deploying HOTPin, Nick has managed to lower helpdesk calls as there is no longer a hard token to be lost or damaged. Provisioning HOTPin is easier and extending the number of users is as simple as adding additional licenses to the software that runs on the WSA appliances.

The increased flexibility that is provided by the solution would be nothing without control. Data leakage is a concern for all IT professionals and Nick is no different. IAG2007 provides the ability to check the security status of an endpoint device and to determine the extent to which it complies with centrally held security policies for remote access. Failure to comply with minimum security policy may result in the user being granted access to a limited number of applications or even to view applications on a read only basis, such is the granularity of the policy setting.

Installation

Nick commented on how easy the installation was. “The Celestix appliance really simplified the deployment of the remote access solution. The appliance was on the network in a matter of minutes and the Celestix web interface made the appliance easy to configure, administer and manage. The Celestix Engineer was excellent at guiding us through how to publish applications to the portal, as well as create lists of authorised users and create some very granular access control policies. The Celestix WSA appliance integrated with our existing RSA two factor authentication

solution perfectly, as well as allowing the use of HOTPin, Celestix own two factor authentication solution. We have now ensured that our remote access solution is not only feature rich, but secure as well.”

Benefits

Time and Cost Savings

- Time has been saved for the remote users and the ICT team. The ICT team now has fewer calls from remote users and can focus more time on other areas of their service.
- Employees feel secure and trust the solution to always give them access to their applications when needed.
- HOTPin has reduced the cost for two factor authentication which has freed budget to be spent in other areas of Suffolk Support Services.
- 1000 users of HOTPin costs considerably less than hardware token based solutions and has saved Suffolk tens of thousands of pounds whilst providing the same level of strong authentication.

Strong Security

- Celestix WSA SSL VPN appliance with Microsoft IAG 2007 includes features that give Suffolk Mental Health Trust strong application security which is vital for patient confidentiality.
- WSA appliances with Microsoft IAG protect the Trust by running end-point assessments of the user's device before access is allowed.

Once a remote session is finished, all traces of the session and all data and passwords are wiped from the endpoint to ensure data is secured at all times and cannot be viewed by other parties.

For further information on Celestix product range please go to: www.celestix.com Or Email: sales@celestix.com

“Infinitely more flexible”



©1999-2010 Celestix Networks Inc. All Rights Reserved. Celestix and Celestix logo are trademarks of Celestix Networks, Inc. Microsoft, Active Directory, Windows, Windows NT and Windows logo are either trademarks registered trademarks of Microsoft Corporation in the United States and/or other countries. All other products and company names mentioned are trademarks or registered trademarks of their respective owners.