©2005-2013 Accops Ltd. All rights reserved.

The information contained in this document represents the current view of Accops Ltd. on the issues discussed as of the date of publication. Because Accops Ltd. must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Accops Ltd., and Accops Ltd. cannot guarantee the accuracy of any information presented after the date of publication.

This white paper is for informational purposes only. ACCOPS LTD. MAKES NO WARRANTIES, EXPRESS OR IMPLIED, IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording or otherwise) or for any purpose, without the express written permission of Accops Ltd.

Contact Accops Ltd. Email:

info@Accops.com

Call +44 (0)1904 567760
# CONTENTS

Accops HySecure INSTALLATION.................................................................4
Accops OS..................................................................................................4
Accops HySecure Virtual Appliance ..........................................................4
Accops HySecure Software ISO.................................................................4
Steps for Installation of Accops HySecure ISO.........................................5
Configuration of Accops OS.......................................................................6
    Network Configuration........................................................................6

BASIC ACCOPS HYSECURE CONFIGURATION........................................9
    Service States.....................................................................................9
    Boot strap State ................................................................................9
    Configuration State...........................................................................9
    Run State..........................................................................................9
    New HySecure Installation..................................................................10
    Bootstrap State .................................................................................10
    Configuration State...........................................................................13
    Sign Into HySecure Server................................................................18
    HySecure Web Portal.........................................................................18
    HySecure Desktop Client....................................................................19
    Change to RUN State..........................................................................20

SETTING UP SECURITY...............................................................................21
    Add Authentication Server..................................................................21
    Add Domain Authentication Server....................................................21

ADDING AN APPLICATION.......................................................................24
    Add Accops TSE as an Application......................................................24
    Example Configuration........................................................................24

    Add Applications to an Application Group...........................................26

CREATE ACCESS CONTROLS....................................................................28
    Give AD Group access to TSE.............................................................28

SIGN-IN AS A DOMAIN USER TO HYSECURE........................................28
    HySecure Web Portal.........................................................................28
    HySecure Desktop Client....................................................................29
CHAPTER 1

ACCOPS HYSECURE INSTALLATION

ACCOPS OS

Accops OS 4 is a security hardened, enterprise class Linux Distribution derived from CentOS. Accops OS hosts the required services for running Accops HySecure Server and is maintained by Accops Development Team.

When installed, Accops OS has a small menu driven interface to manage host configuration like network settings modifications or reinstallation of firmware.

Accops OS comes on an integrated installer CD or bootable USB drive. The integrated installer is a single click OS installer which also installs the HySecure software.

NB: Installing the Accops OS will erase all existing data off your system without asking about details of partition.

Accops HySecure is available as a virtual appliance as well as a software only option.

ACCOPS ONEGATE VIRTUAL APPLIANCE

Accops HySecure is available in Open Virtualization Format (OVF) which is an open standard for packaging and distributing virtual appliances to be run in virtual machines. The standard describes an ‘open, secure, portable, efficient and extensible format for the packaging and distribution of software to be run in virtual machines’. The OVF standard is not tied to any particular hypervisor or processor architecture. The unit of packaging and distribution is a so called OVF Package which may contain one or more virtual systems each of which can be deployed to a virtual machine.

The Accops HySecure Virtual Appliance has been verified with VMware ESXi. The Virtual Appliance is downloadable from the Accops Website (http://www.Accops.com). Simply extract the image file and import directly into your VMware environment and you are ready to go.

All the functionalities of the virtual appliance are the same as the software version.

ACCOPS ONEGATE SOFTWARE ISO

Accops HySecure is also available as software installer. This single click integrated ISO image installs both Accops OS and Accops HySecure on any custom hardware. The installer ISO can be downloaded from the Accops Website (http://www.Accops.com).

Accops OS is a CentOS based platform, hence any hardware that supports the Linux distribution is supported by Accops OS. Accops OS is available in 64-bit versions.

The functionalities of the HySecure platform are the same irrespective of the underlying platform. Both versions ship with a system default evaluation license allowing 5 users for 30 days.
**STEPS FOR INSTALLATION OF ACCOPS HYSECURE ISO**

Installing the Accops HySecure server from the ISO installer is simple. Either burn the ISO to CD or if you are installing in a virtual environment simply mount the ISO inside the virtual machine.

1. The installer screen will appear as shown. If you are installing through USB, type USB otherwise press Enter.

![Installer Screen]

2. Installation will start automatically and will take approximately 10 minutes to complete, depending on hardware.

![Installation Progress]

3. After completion of Installation, remove CD and restart the machine.
After completion of installation and restart you will get a prompt to login to gain access to the Accops OS Console menu. This is also the first stage of configuration you will see if using the Virtual Appliance.

The account name is **consoleadmin**. The default password for the account is **adminconsole**. The administrator has option to change the password for consoleadmin user. Root access to Accops OS is blocked completely. Once authenticated you will see the following Accops OS Console screen:

Choose a number for the configuration option you require. To get started ensure you configure the server with an IP address which you can access from a browser on your PC.

**NETWORK CONFIGURATION**

In this screen you can configure the network settings for your HySecure server.

---

**NB:** Accops HySecure installs with a default static IP address of 192.168.1.100.
The HySecure virtual appliance ships with 2 Ethernet interfaces as standard setting the second NIC as DHCP enabled.

The most common configuration scenarios for Accops HySecure are shown below. Depending on your chosen network configuration you will need to setup your network interfaces to suit.

![Diagram of network configuration]

**CONFIGURE ETHERNET DEVICE**

In the Ethernet configuration screen, select the number of the NIC you wish to configure. For example:

To configure the `eth1` interface in the screen below simply type 1 then hit Enter.

```
--- ETHERNET CONFIGURATION ---
Following Ethernet devices found on the system.
et0 [DHCP] [UP] 172.17.4.253
---
Enter the device number to configure it (8 to return):  
```

Select 1 to manually configure NIC or 2 to configure DHCP option.

```
--- ETHER Configuration ---
ETH0 DETAILS:
PROTOCOL: DHCP
IPADDR: 172.17.4.253
NETMASK: 255.255.255.0
DEFAULT GATEWAY: 172.17.0.1
---
1) Manually configure ETH0
2) Configure DHCP for ETH0
R) Return to previous menu
Select one of options above: 
```

Enter the relevant IP information when prompted and choose y to apply the configuration. The network service will restart and you will be prompted to press a key to continue when it is finished.

**NB:** Configuring HySecure with static IP is always good practice.
SET HOSTNAME

In this screen the administrator can configure the HySecure server hostname.

To configure the hostname choose option 2 then type the fully qualified domain name that users will use to access this HySecure server and press Enter. Press any key to continue.

Important: Accops HySecure resolves requests only through hostname. The hostname should set before starting configuration. If you are changing hostname after configuration this will affect your whole set up and you will need to re-configure.

For instructions on all other commands available from this console please consult the HySecure Administrator’s Guide.

Important: Accops HySecure server does not require the administrator to have root access to the underlying operating system. All installation and configuration can be performed using both the Accops OS Console (shown above) or through the web based management console. Accops Support team may require shell access for advanced troubleshooting but this is not common.
CHAPTER 2

BASIC ACCOPS HYSECURE CONFIGURATION

SERVICE STATES

The HySecure server has three states:

1. Boot strap
2. Configuration
3. Run

BOOT STRAP STATE

Immediately after install the HySecure server is in System Configuration state, also known as boot-strap state. During this stage, admin configures the system settings, including network, license and certificate settings.

During this stage the first security officer account is created.

CONFIGURATION STATE

In this state, the HySecure server is in configuration mode. It will not accept connections from any user other than Security Officers and Administrators.

Once bootstrap state is complete, the server automatically moves to Configuration state.

Administrators can bring the server from run state to configuration state from administrator console for performing system wide changes.

RUN STATE

In this state, the HySecure server is fully functional. No critical system wide changes can be performed on the system during run state.

HySecure server does not move automatically from configuration state to run state after a fresh configuration. To change from configuration state to run state, you should go to VPN Status > VPN Server State page in the management console and switch to Run State.
NEW ONEGATE INSTALLATION

BOOTSTRAP STATE

After a new installation of Accops HySecure, the system is running in bootstrap mode. Follow these steps to complete bootstrap stage.


2. Click on the link Manage VPN Now

3. Read and click the box to accept the Software License Agreement.

4. The Accops HySecure – System Configuration screen appears where you can specify host, network interface and date and time settings for the server. Confirm the settings and click Submit.

5. Click OK on the message and Continue to confirm the settings configuration.
6. At this stage you are prompted to select the HySecure installation type. Choose from the default Standalone server, Clustered server (see Administrators Guide for more information on High Availability options) or Restore a previous server configuration.

   **Stand Alone installation** will create a new instance for installation in new environments but if you have a previous system backup from which you wish to recover then select **Restore complete configuration from Backup file** then Click Continue.

   **NB**: For full system backup and restore to work, the hostname should not change across backup and restore.

On completion of System Configuration, the HySecure server continues through Bootstrap stage, and is ready for a one-time registration process. In Bootstrap State, first Security Officer Registration, SMTP Server configuration, Database User configuration, and several others tasks are completed, including:

- Register first Security Officer
- Create Root Certificate Authority (CA) Certificate
- Register SSL Certificate for VPN
- Create Signer Certificate
- Create Verifier Certificate
- Create VPN database and database tables
• Register VPN Ports and Apache Ports (port 80/443, 4001, and 4002)
• Create Configuration files
• Enter Configuration State (this change occurs automatically after the Bootstrap process is complete)

The tasks such as creating CA certificate, Signer Certificate, Verifier Certificate, and many others take place internally when you register the necessary details with server during server Bootstrap.

1. Once all of the internal tasks have been completed you will be redirected to the Certificate Authority screen.

2. In the Certificate Authority Mode section the Default Propalms Internal CA field is chosen by default. This enables the server to act as Certificate Authority. Choose External CA if you wish to use a 3rd Party Certificate Authority.

3. Click the Submit button to save the changes made. On clicking the Submit button, the Certificate Authority page appears as shown below depending on which option you selected.

   a. For External CA provide CA Certificate path, CA Private Key path and CA Private Key Password.

   b. For Accops Internal Certificate Authority fill out the required fields
c. You also need to create the Security Officer account on the HySecure server. This account provides administrator access to the HySecure management console where further accounts can be created. See table below for description of each field.

<table>
<thead>
<tr>
<th>FIELD</th>
<th>VALUE</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Certificate Authority Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Company Name</td>
<td>&lt;Company Name&gt;</td>
<td>Name of the company to which Certificate will be issued.</td>
</tr>
<tr>
<td>Country</td>
<td>&lt;Country Name&gt;</td>
<td>Name of the country where Certificate will be issued.</td>
</tr>
<tr>
<td>State</td>
<td>&lt;State Name&gt;</td>
<td>Name of the state where Certificate will be issued.</td>
</tr>
<tr>
<td>City</td>
<td>&lt;City Name&gt;</td>
<td>Name of the city where Certificate will be issued.</td>
</tr>
<tr>
<td>Validity (days)</td>
<td>&lt;No. of Days&gt;</td>
<td>Validity period for the Certificate Authority.</td>
</tr>
<tr>
<td>Security Officer Account</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Name</td>
<td>&lt;First Security Officer Name&gt;</td>
<td>Full name of First Security Officer.</td>
</tr>
<tr>
<td>Email</td>
<td>&lt;Username@domain name&gt;</td>
<td>Email address of First Security Officer.</td>
</tr>
<tr>
<td>User ID</td>
<td>&lt;User Name&gt;</td>
<td>Basic Authentication Login ID for First Security Officer.</td>
</tr>
</tbody>
</table>

4. On clicking the Submit button, the following screen confirming the registration will appear after a short while. Accops HySecure Server will attempt to email the Root Certificate (cacert.cer) and the Passphrase to the first Security Officer's e-mail address specified. However, it is recommended to leave this page open or copy the passphrase in case this email isn't received. You will need the passphrase in order to enroll the first Security Officer Account and login to the management console.

First Security Officer ACCOPS Certificate User registered successfully. The Passphrase is K0BH85X10R05FN14

Please follow these steps:
1. Download the Propalms HySecure Client from HySecure home page.
2. Enroll yourself with the help of the Passphrase provided above.
3. Login Into Propalms HySecure.
4. Open the HySecure Management Console.
5. Change the HySecure server state to "RUN" mode at 'Server Configuration' -> 'Server State'.

13
CONFIGURATION STATE

Upon successful completion of Bootstrap State, the server automatically moves into Configuration State. The following tasks are completed in Configuration State:

- Enroll First Security Officer
- Move HySecure from Configuration State to Run State

NB: User Registration and User Enrollment are two different processes. During the User Registration process, the User Name and User E-mail Address are registered with VPN and a Passphrase is generated. During the User Enrollment process, the Passphrase and a Password, supplied by the User, are registered with VPN, and a user Certificate file (.cer) is generated.

Applications can be added to the HySecure server when it is in Configuration State. However, users cannot access applications until the server is in Run State.

HySecure server sends an email to the first Security Officer account as registered previously, containing a Root Certificate, Passphrase, and a link to the HySecure home page. The Security Officer can save the Root Certificate file (cacert.cer) in a local folder and import it to the list of Trusted Root Certification Authorities in the browser to avoid seeing warnings when authenticating.

ENROLL USING WEB PORTAL

NB: In this example we are using a Windows 8 PC running Internet Explorer 10. You can also use Google Chrome and Firefox if you wish.

The first Security Officer, whom you registered in the HySecure Bootstrap State section earlier, must now be enrolled using the Passphrase available in the e-mail generated automatically and sent to the first Security Officer account. The password required must be supplied by the first Security Officer. When the Security Officer is successfully enrolled, a user Certificate is imported to the local personal certificate store.

NB: Java is required to run the HySecure web portal. When you access the portal you will be prompted to download and install Java if you do not already have it enabled in your browser.

2. Click on the link Sign in Now.
   NB: You will probably get a browser certificate warning; you can ignore this and continue
3. You will receive a browser notification that the webpage wants to run Java. Choose Allow.

You may also receive a Security warning about the HySecure portal’s SSL certificate at this stage. Choose to Trust content from this publisher and click Yes.

4. On the Sign-in page click Login with SSL client certificate. This will prompt you to run the webmgrapp from the HySecure portal. Choose Always trust content from this publisher and click Run.

5. It may take a moment for the Java Platform to initiate. Click the Enroll your SSL certificate link.

6. In the Pass Phrase field, type the Passphrase you received in the e-mail (if you prefer copy and paste the Passphrase from the e-mail to this field).

In the Password field, type a password for your Security Officer Account. In the Confirm Password field, retype the password for confirmation. Click on Submit to submit the enrollment information and click on Cancel to exit from this screen without saving the changes.
7. You should now see your certificate user listed in the **Client Certificate** field. Simply enter your chosen password to Sign in and access the HySecure Administration Console.

---

**ENROLL USING DESKTOP CLIENT**

1. To download and install the Accops HySecure desktop client, launch the web browser and go to URL [http://HySecure_gateway_ip_address/](http://HySecure_gateway_ip_address/) or [http://<HySecure_hostname>/](http://<HySecure_hostname>/)

2. Choose the **Windows Client** from the Download Desktop VPN Client section.
3. When prompted to, Save the **Accops HySecure client installer**. Go to the location where you saved the file and right click and choose **Run as Administrator**.

![Image of File Save and Run Options]

4. Double click the desktop icon for **Accops HySecure Client** to start the desktop client. In the Server box type the name of your HySecure server and choose **Login with a digital certificate**.

**NB:** if you receive a SSL certificate warning click yes to continue. The client can be configured to suppress these warnings in future.

5. On the Action menu click **Enroll Client SSL Certificate**.

![Image of Enroll SSL Certificate Process]

In the Passphrase field, type the **Passphrase** you received in the e-mail (if you prefer copy and paste the Passphrase from the e-mail to this field).

In the **Password** field, type a password for your Security Officer Account.

In the **Confirm Password** field, retype the password for confirmation.

Click on **Submit** to submit the enrollment information and click on **Abort** to exit from this screen without saving the changes.
Once enrolled you can sing in and access the HySecure Administration Console.

**ENROLL SECOND SECURITY OFFICER AND ADMINISTRATORS**

After the first Security Officer is successfully enrolled, he or she can register a second Security Officer and any Administrator accounts.

Once registered, the second Security Officer and the Administrators must enroll themselves, following the steps above, substituting the second Security Officer and Administrator data accordingly.

**SIGN INTO HYSECURE SERVER**

As previously documented, there are two primary way to sign in to Accops HySecure; Web Portal and Desktop client. Accops HySecure supports two types of Authentication Mechanisms to access services over the network:

- **Basic Authentication:** This is a weaker authentication mechanism. Users sign in using User ID and Password. The Low Security Users are authenticated with this mechanism.

- **Certificate Authentication:** This is a stronger authentication mechanism. Users sign in with Certificate and Password. Security officers and Administrators are also authenticated with this mechanism.

To login as a Security Officer, choose **Login with SSL certificate**; the security officer certificate associated with your HySecure server should automatically be shown in the certificate field.

Type the **password** for the Security Officer Account and click **Sign in**.

The landing page presented to the user depends on the logon method chosen.

**HYSECURE DESKTOP CLIENT**

You launch the HySecure desktop client from the Accops HySecure client icon on your desktop or start menu. Choose **Certificate User** if logging in as a Security Officer, Administrator or High Security User.
Once authenticated you are presented with the Application List which shows any Web Applications published to the user. If you have logged in as a Security Officer or Administrator account you can click on VPN Management Console link in order to continue setting up the HySecure server.

With both of these logon methods you will also notice that a HySecure icon is placed in the system tray providing access to extra client options.

**CHANGE TO RUN STATE**

In order to access HySecure as a non-admin user a Security officer or Administrator needs to move the server into RUN state. This is performed in the Management Console under VPN Status > VPN Server State. Simply click Run State to change the status.
Open HySecure management console, click to expand Auth Management, and then click Authentication Servers. Click Add to specify a new Authentication Server. Choose AD/LDAP to add a domain authentication server.

Type an identifier of the External AD/LDAP Authentication Server in Server Name field.

Type the IP address, host name, or FQDN of the AD/LDAP server, in the Host Name field.

The default LDAP port number is displayed in the Port field. Please note that you can change this port number as needed.

Type the admin bind DN in the Admin Bind DN field e.g. cn=vpnadmin,cn=Users,dc=prodemo,dc=local

Type your password in the Admin Password field.

Type the base DN in the Base DN field e.g. dc=prodemo,dc=local

User search attribute is given in the User Search Attribute field, e.g. samAccountName.

User Group search attribute for the server is displayed in User Group Search Attribute field, e.g. MemberOf.

NB: The User Group Search Attribute is used to obtain the User Groups from AD/LDAP server.
Click **Test Connection** to verify the configuration. If this is successful then click **Submit** to save the configuration data or **Reset** to clear all data from this screen.

AD/LDAP Configuration info updated successfully message will be displayed.

**SPECIFYING AUTHENTICATION DOMAIN**

To quickly add your domain as an authentication server open the Management Console and expand **Auth Management**. Click **Authentication Domain** from the submenu and select the **DefaultDomain** in the list of domains and choose **Modify**.

If you wish to login as Native users (local users on HySecure server) as well as Domain users then click to **Add another Authentication Server**.
Change your domain authentication servers to Priority 1 by using the drop down menu.

You can delete servers from the priority list by using the **Delete Server** option.

Click **Submit** when you have finished.

**NB:** Deleting servers from this list does NOT remove the authentication servers from the system.
CHAPTER 4

ADDING AN APPLICATION

Accops HySecure supports a wide range of multi-port TCP/UDP applications. The following sections will take you through adding Accops TSE/VDI as an application and providing user access. For more in depth information on adding applications see Accops HySecure Administrator’s Guide.

ADD ACCOPS TSE AS AN APPLICATION

Accops HySecure seamlessly integrates with Accops TSE allowing secure access to TSE applications through the gateway. HySecure can be used as a replacement for the Single Port Relay service that is built into TSE allowing greater scalability, security and stability.

Once a user logs into HySecure, if there is a Accops TSE LaunchPad application assigned to them then they are authenticated to TSE using their HySecure credentials and seamlessly delivered access to their authorized TSE applications. How this is presented to the user is dependent on the method of access.

Go to Access Management > Applications and choose Add.

EXAMPLE CONFIGURATION

Create application rules for TSE following these examples.

You need to create a TSE Application Server (RDP) rule for each TSE App server role installed. If TSE Printing is used then a TSE Print rule is required for each app server also. HyperPrint does not need this rule for it to work.
ADD APPLICATIONS TO AN APPLICATION GROUP

Application Groups make it easy to combine multiple application rules together which makes it easier to allow provide HySecure users access to these resources.

Go to Access Management > Application Groups and choose Add.

Give the Application Group a name and click Select Applications. In the above example we are adding a TSE Application Group called TSE_ACCESS.

Select the relevant Applications to be included in the Group and add them to the Selected Applications list. Replace TSE with VDI for providing access to VDI desktops.

NB: The High Security Level is for certificate based authentication users.
Select the Applications you wish to add to the group by clicking on them on the Applications panel. Choose Add to make them a member of the Application Group. Click Submit to finish.
CHAPTER 5

CREATE ACCESS CONTROLS

Access Controls manage the availability of services/applications to users in accordance with corporate policies. Access Controls are primarily specified for user groups, although in HySecure they can now be based on Device ID and Endpoint Protection also. Through HySecure Access Controls, a user group is assigned one or more Application Groups as needed.

When a user logs on, the Access Control Lists specified for the User Groups to which he/she belongs are activated so that the user can have access to permitted applications.

GIVE AD GROUP ACCESS TO TSE

Go to Access Management > Access Controls and choose Add.

Give the Access Control a name and optionally a description.

From the Select Authorization Server dropdown choose your domain authentication specified earlier. You will notice that the High Security and Low Security options are hidden when choosing Domain authentication instead of local/native.

Under Access Control Type, specify Application so that you can see a list of the Application Groups you have created.

Add the relevant Domain Groups from the Select User Group panel.

Add Application Groups that you want to provide these users access to under the Select Application Group Panel.

Leave the Access Control enabled and click Submit.

Repeat for VDI if access to Accops VDI hosted desktops is required.
NB: When using native authentication and a High Security User logs on with Certificate and Password, the Access Control Lists specified for the subscribed HS Users Groups are activated. And when he/she logs on with Login ID and Password, the Access Control Lists specified for the subscribed BA User Groups are activated.
CHAPTER 6

SIGN-IN AS A DOMAIN USER TO HYSECURE

HYSECURE WEB PORTAL

Accops HySecure Portal is a browser based access mode. You can access the portal by either browsing to http://HySecure_gateway_ip_address/ or http://<HySecure_hostname>/ and choose Sign in Now link. Alternatively users can browse directly using https:// and the portal login will appear directly.

Simply enter your domain credentials to authenticate to the HySecure portal. These credentials will be used to sign you in to TSE also. When logging in through the HySecure Web Portal with TSE application assigned, the user will see an extra tab on the portal named TSE Applications. This page will display the TSE applications that have been published to this user from the TSE Management Console.

If your Windows Client does not have the TSE client installed you will be prompted to download and install the latest client...

The default URL for the TSE client download is from the Accops Website, you can change this to a custom location under Host Configuration > Client Settings > TSE Client Settings in the HySecure Management Console.
When logging in through the HySecure Web Portal with VDI application assigned, the user will see any virtual desktops available to them listed under **VPN Applications > Accops Virtual Desktops**.

### HYSECURE DESKTOP CLIENT

To download and install the Accops HySecure desktop client, launch the web browser and go to URL [http://HySecure_gateway_ip_address/](http://HySecure_gateway_ip_address/) or [http://<HySecure_hostname>/](http://<HySecure_hostname>/). Choose the client for your operating system from the **Download Desktop VPN Client** section.

When prompted to, Save the **Accops HySecure client installer**. Go to the location where you saved the file and right click and choose Run as Administrator.
Login as a domain user account by simply entering your domain username and password and the client will sign-in to HySecure and pass-through these credentials to TSE automatically.

When logging in through the HySecure desktop client with TSE integration the user will be presented with the **HySecure Application List** displaying their published TSE applications among any other HySecure Apps they have been provided.

If the user logs into the HySecure server using desktop client with VDI integration configured then the Application List will display their VDI Desktop under the Virtual Desktops section.

Accops Ltd is a global provider of application delivery and secure remote access solutions for Remote Desktop Services and Virtual Desktop Infrastructures. Delivering to Enterprises of all sizes we offer reliable, scalable and affordable solutions that simply work. Our belief is that application delivery solutions should be flexible, dynamic and above all, simple to use.