globalscape®
securely connected

EFT™ CLOUD

IMPLEMENTATION GUIDE

Microsoft Azure
Amazon Web Services

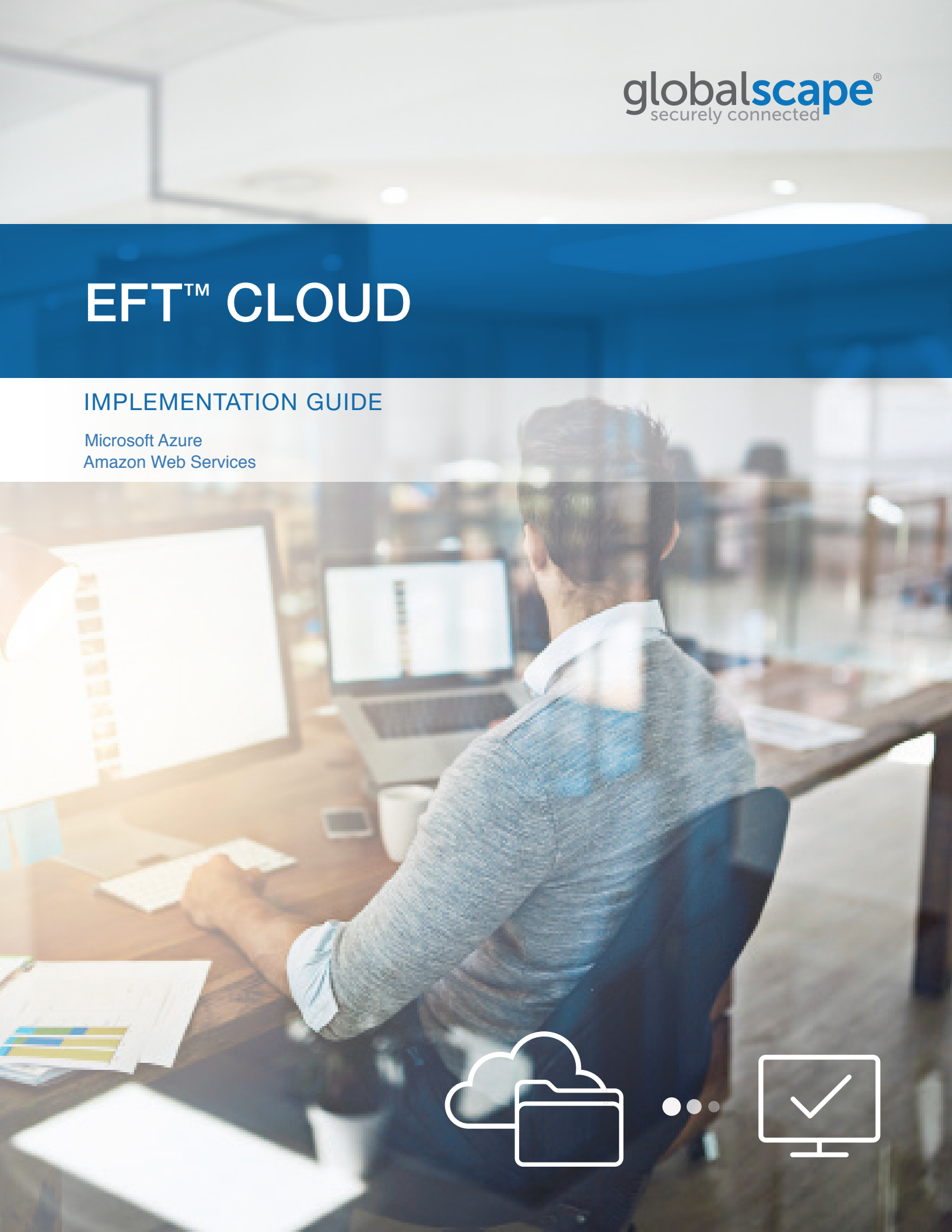

TABLE OF CONTENTS

DEPLOYMENT OPTIONS

Aside from Globalscape's SaaS solution, EFT Cloud Services, we also offer EFT that you can deploy yourself, in the cloud, with a perpetual EFT license and by a managed service provider (MSP), Globalscape, or by yourself. EFT can be installed on:

- Amazon Web Services (AWS)
- Microsoft Azure
- An MSP of your choosing

No matter how you deploy EFT, you can request a Technical Account Manager (TAM) to administer EFT for you.

DEPLOYING AMAZON EC2 INSTANCES OF EFT ON AMAZON WEB SERVICES (AWS)

You don't need to have your own infrastructure and server hardware to deploy an enterprise-level managed file transfer (MFT) server. As an alternative, or an adjunct, to EFT installed on premises, EFT can be installed on Amazon Web Services, Microsoft Azure, or other hosting providers, with a perpetual license and managed by a managed service provider, a Globalscape Technical Account Manager (TAM), one of our partners, or yourself. This guide explains how to deploy EFT on Amazon Web Services.

PREREQUISITES

To run EFT on AWS, you need the following:

- An Amazon AWS account
- A license key from Globalscape if you plan to use EFT past the 30-day evaluation period.

Licensing

The EFT image includes a fully functional, preconfigured copy of EFT that will operate without a license for 30 days. After the evaluation period is over, you will need to provide a license key to continue using the software. The license key is not restricted to an EFT running on AWS, but is instead restricted based on the number of servers licensed. For more information on licensing, please refer to EFT's End User License Agreement or contact Globalscape sales.

Obtaining the Image

If you haven't done so already, log in to your AWS account, go to the AWS marketplace, and search for "Globalscape." Locate the Globalscape EFT offering, select it, and then follow Amazon's One-Click setup process to create and launch an instance of that image. Globalscape recommends that you select the default options, and also requires that RDP be available (so you can log in and perform administrative tasks in EFT), and HTTPS (so you can log in as a user and upload and download files to EFT using EFT Web Admin).

Quick Test

If you used the One-Click setup, then an instance of EFT is both created and launched in a single step. Give the instance a few minutes so that the machine password will be available and so that EFT can finish configuring itself. After 5 minutes or so do the following to connect to EFT:

1. In your web browser, type:
   https://<this_instance_ip_address>

If the connection fails, then you should either try again in a few minutes, or double check the Security Group (EC2 Dashboard > Network & Security > Security Groups) assigned to this image, ensuring that HTTPS is added and that your IP address is allowed.

2. If you get a security warning in your browser, select the option to proceed. The browser is simply alerting you to the fact that the SSL certificate used by the site is unsigned (self-signed), and thus untrusted. More on SSL certificates below.
3. At the login page, type in the user account credentials as follows:

   Username: ec2-user
   Password: <The_Instance_ID>

4. The instance ID is shown in your EC2 Dashboard for this instance. This is a unique value that was generated when you created the instance from the EFT image. When the instance was launched for the first time, a script was run that generated this test account and retrieved the instance ID, and thus dynamically setting the password. Even though it is unique, we recommend you change the test user account credentials at the earliest opportunity, as both the testuser and EFT administrator account are assigned the instance ID as their respective password.
5. In the rare case that the script failed and your login fails, then please contact our support team or RDP in and use EFT's administration interface to manually configure EFT.
6. When login succeeds, then EFT's Web Transfer Client (WTC) interface appears, and you will be able to transfer files from/to EFT using the intuitive controls provided.

The WTC represents a tiny sub-set of EFT's functionality, and isn't necessary if purely automated transactions will be conducted between systems; however, it is a good way to test that the server is running. The WTC is useful when person-to-business or person-to-person transfers are needed.

EFT Administration

To take full advantage of EFT you will need to configure it beyond the preconfigured settings. This includes security settings that meet your internal policies, user provisioning, and creation of workflows that depend on triggers such as files being uploaded, files deposited into a "hot" folder, or recurring scheduled events.

1. Establish a remote desktop session to the running instance (if you are reading this then you are likely already connected). Instructions for RDPing and for obtaining the uniquely generated administrator password for this instance are available on Amazon's website.
2. Once logged in to Windows, click on the EFT administration shortcut located on the desktop.
3. When the administration interface appears, you will be asked which server you want to administer. Select **Local server**, then click **OK** or **Next**.
4. On the next screen, provide your administrator credentials as follows:

   Admin username: Administrator
   Password: <The_Instance_ID>

5. As with the test user account, the admin account uses the instance ID as the password. We highly recommend that you change the default password, which can be done on the Server's Administration tab. (Click the Server node in the tree pane.)

6. You can now configure the server to your liking, which could include things like adding more users to the default Site, creating a new Site (which is like a virtual host that can have its own unique authentication mechanism, protocol, and security settings), changing default settings, or start experimenting with EFT's automation capabilities, which include the Event Rules and Advanced Workflows features.
7. The complete documentation on EFT administration can be found on our support website.

Next steps

1. First, don't forget to change your EFT administrator and ec2-user account passwords in EFT.
2. If you haven't done so already, you should change your Windows Administrator password.
3. Enable additional protocols in EFT (FTPS, SFTP, AS2) as desired, remembering to update your AWS Security Group values as necessary, so that connections can be established from outside of AWS.
4. EFT was preconfigured with Amazon's SMTP server values; however, you will need your Amazon Simple Email Service (SES) SMTP credentials (http://docs.aws.amazon.com/ses/latest/DeveloperGuide/Welcome.html) if you want to leverage EFT's email notification capabilities.
5. If you plan on using this EFT in a production environment, and assuming it's been licensed, then do not forget to replace the test SSL certificate that was generated for EFT with a CA signed certificate. Please note that the test certificate private key password was also the instance ID.
6. If you plan on using this EFT in a production environment, then you will probably want to audit to a separate SQL server, rather than the provided SQL Server Express 2014 edition. In order to both change EFT's audit settings AND create the schema on the target SQL server, you will need to re-run the installer, choose **Modify**, and then follow the instructions when prompted to set EFT auditing and reporting. Alternatively you can contact our support team for assistance.
7. The instance will default to the UTC time zone. Instructions for changing the time zone here: http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/windows-set-time.html
8. You can join this instance to your AWS domain within your Virtual Private Cloud (VPC) by following these instructions: http://docs.aws.amazon.com/AWSEC2/latest/WindowsGuide/ec2-join-aws-domain.html Note that EFT supports an authentication mode that lets you point to an AD controller, using native Windows calls (for full impersonation), using LDAP, if authentication alone is needed (with EFT controlling authorization).

Contact the Globalscape sales team if you would like to see a demo or have specific questions about deploying EFT on AWS.

The Amazon EC2 Instance Deployment Guide.pdf provides the steps necessary to create EC2 – Virtual Servers in the Cloud instance. Note that Amazon charges a fee for this service, and the fee increases with the amount of bandwidth you need.

DEPLOYING EFT ON MICROSOFT AZURE

You don't need to have your own infrastructure and server hardware to deploy an enterprise-level managed file transfer (MFT) server. Instead, you can build and scale EFT on Microsoft Azure. The instructions below describe how to get started with this type of cloud-based deployment.

Prerequisites

To run EFT on Azure, you need the following:

- An Azure account
- An EFT license key if you plan to use EFT past the 30-day evaluation period

Licensing

The EFT image includes a fully functional, preconfigured copy of EFT that will operate without a license for 30 days. After the evaluation period is over you will need to provide a license key in order to continue using the software. The license key is not restricted to an EFT running on Azure, but is restricted based on the number of servers licensed. For more information on licensing please refer to EFT's End User License Agreement or contact Globalscape sales.

Create VM

If you haven't done so already, log on to your Azure account, go to the Azure marketplace, and then search for "Globalscape." Locate the Globalscape EFT offering, select it, and then click **Create**. Specify your desired configuration settings, and make note of the admin username and password you enter, as you will need them later. Click **Purchase** to deploy an instance of EFT. Azure's setup process will create and launch an instance EFT, which could take several hours.

Quick Test

Once the image has been deployed:

1. In your web browser, type https://<instance_ip_or_host_address>. If the connection fails then you should try again in a few minutes.
2. If you get a security warning in your browser, select the option to proceed. The browser is simply alerting you to the fact that the SSL certificate used by the site is unsigned (self-signed), and thus untrusted. More on SSL certificates below.
3. At the login page, type in the user account credentials as follows:

   Username: testuser
   Password: Alaska!!
4. You will be prompted to change the test account's password upon initial login.
5. In the rare event that the EFT setup script failed and the login fails, then please contact our support team or RDP in and use EFT's administration interface to manually configure EFT.
6. When the login succeeds, then EFT's Web Transfer Client (WTC) interface appears after a few moments, and you will be able to transfer files from/to EFT using the intuitive controls provided. The WTC represents a tiny sub-set of EFT's functionality, and in fact isn't necessary if purely automated transactions will be conducted between systems; however, the WTC is a good way to test that the server is running, and is useful when person-to-business or person-to-person transfers are also needed.

EFT Administration

To take full advantage of EFT you will need to configure it beyond the preconfigured settings. This includes security settings that meet your internal policies, user provisioning, and creation of workflows that depend on triggers such as files being uploaded, files deposited into a "hot" folder, or recurring scheduled events. To configure EFT:

1. Establish a remote desktop session to the running instance. From the Azure portal, select the virtual machine you created and click the **Connect** icon. Type in the administrator username and password you typed in when creating the image.
2. Once logged in to Windows, click on the EFT administration interface shortcut located on the desktop.
3. When the administration interface appears, you will be asked which server you want to administer. Select the Local server and then click **OK** or **Next**.
4. On the next screen, click **Windows Integrated Authentication** and then click **Connect**.
5. Once connected to EFT's administration interface, configure EFT to your liking, which could include things like adding more users to the default Site, creating a new Site (which is like a virtual host that can have its own unique authentication mechanism, IP mappings, protocols, and security settings), changing default settings, or start experimenting with EFT's automation capabilities, which include EFT's powerful Event Rules and Advanced Workflows features.
6. The complete documentation on EFT administration can be found on Globalscape's support website.

Next steps

1. If you plan on using this EFT in a production environment, and assuming it's been licensed, then do not forget to replace the test SSL certificate that was generated for EFT with a CA-signed certificate. Please note that the test certificate private key password was a large random number that cannot be recovered.
2. If you plan on using this EFT in a production environment, then you should audit to a separate SQL server, rather than the provided SQL Server Express edition. In order to both change EFT's audit settings AND create the schema on the target SQL server, you will need to re-run the installer, choose Modify, and then follow the instructions when prompted to configure EFT auditing and reporting. Refer to the EFT online help or contact our support team for assistance.

Please contact our sales team if you would like to see a demo or have specific questions you would like answered.

For more information please go to:
www.globalscape.com

globalscape®
securely connected

GlobalSCAPE, Inc. (GSB)
Corporate Headquarters
4500 Lockhill-Selma Road, Suite 150
San Antonio, TX 78249 USA
Sales: 210-308-8267 / Toll Free: 800-290-5054
Technical Support: 210-366-3993
Web Support: www.globalscape.com/support