**PRIVATE CLOUD (ANCHOR) SETUP INSTRUCTIONS**

Customer Name:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PM Engineer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Date Needed: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

PM Quote Reference:  \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Active Directory Integration?

* Yes
* No

Number of years SSL certificate is applied for:

* 1
* 2
* 3

Cloud Fileshare Package Level Selected:

* Workstation Backup Only
* Fileshare Only
* Fileshare with Workstation Backup

Split DNS in use at client site? (If so, DNS record addition required.)

* Yes
* No

**PHASE 1: STARTING CHECKLIST**

* Lead admin requests customer-branded cloud logo from Mike. CC Robert and Doreyne.
* Lead admin requests branded QuickCard from Doreyne (using customer-branded cloud logo).
* Lead admin requests list of accounts to be created/imported from customer (regardless of Active Directory Integration response).
* Lead admin requests the number of years for which to buy the SSL Certificate, from the Business Office.

**PHASE 2: ANCHOR ORGANIZATION SETUP**

* Go to cloud.planetmagpie.com while logged into the Anchor server (cloudmagpie/10.20.0.49). Log in with admin credentials.
* Click the "All Organizations" tab on the left to highlight it.
* Click "Create Organization" above it.
* Enter the new Organization Name (the company/client name).
* Enter Hostname: cloud.<domain>.com
* In the Contact Email field, enter [anchor@planetmagpie.com](mailto:anchor@planetmagpie.com).
* In the Space Quota field, enter the value corresponding to the selected package (noted above), from 150GB to 750GB.
* Under Organization Policies, change the Max File Size to 800 MB.
* All Policies options are checked by default. Uncheck the ones they don't get depending on package (see checklist above).
* Click Save.
* Next, customize the Organization’s branding.
* Access the Anchor Server via Remote Desktop. In its C:\Support\Logos folder, place the new custom-branded cloud logo. You will find the cloud icon file under C:\Support\Logos\ICO File.
* Within the Anchor Organization, click its Settings tab. Click the Branding button.
  + Select the “Custom branding for this organization” option. Anchor will present you with a number of branding options.
  + Click the Browse button next to “Logo.” Navigate to the C:\Support\Logos folder, and select the new custom-branded cloud logo.
  + Click the Browse button next to “Icon.” Navigate to the C:\Support\Logos\ICO File folder, and select the cloud icon.
  + The Splash Screen is optional. You don’t need to add a file here.
  + Enter the customer’s full company name in the “Company Name” field.
  + Enter the customer’s website URL in the “Company URL” field.
* Click the Save button.
* On the Anchor server, access Network Settings. Open the properties of the “cloud” connection.
* Enter TCP/IP v4 Properties. Under “Advanced”, add another IP address.
* Determine the next available virtual IP from the list (graded up from previous Anchor clouds; 10.20.0.54 is the last one currently used). Enter the virtual IP here. It will serve as the new Anchor organization’s IP.
* Use Subnet Mask: 255.255.255.0
* Click OK until done. The server can now internally answer for that new IP.
* Open the hosts file on the server (as Administrator). Enter in the new IP along with the hostname (for example, “10.20.0.55 cloud.NewOrganization.com”). Use the same pattern as the other hostnames listed.
* Proceed to Phase 3.

**MOVING USERS TO A SECONDARY ORGANIZATION**

You may be asked to move users out of an existing Organization, into a new Organization you create for them. This new Organization will NOT have its own specialized URL, and will not require an SSL cert.

* Go to cloud.planetmagpie.com. Log in with admin credentials.
* Click the "All Organizations" tab on the left to highlight it.
* Click "Create Organization" above it.
* Enter the new Organization Name (the company/client name).
* Leave Hostname field blank.
* Enter a Contact Email (typically [anchor@planetmagpie.com](mailto:anchor@planetmagpie.com)).
* Under Space Quota, adjust amount of space if needed. If you are only moving a small number of users, leave the default.
* Under Excluded Extensions, remove any extensions the customer may use. If unsure, leave as-is and ask the customer if they have any unusual file types.
* All Policies are checked by default. Uncheck the ones they don't get depending on package (see checklist above).
* Click Save.
* \*\*NOTE: These customers will still use the original Organization URL (typically cloud.planetmagpie.com).
* Click the Organization where the users currently reside. Click Accounts.
* Click the Edit button for the user you want to move to the new Organization.
* In its Account Settings window, click the dropdown menu next to Organization.
* Select the new secondary Organization you created.
* Click Save.
* Repeat these steps for all additional users.
* Once the users are in place, click the new Organization. Click Accounts.
* Confirm that all users now show up under Accounts.
* Click Backups. Confirm that any backups assigned to those Accounts transferred as well.
  + If not, you will need to recreate the backups.
* DO NOT proceed to Phase 3.

**PHASE 3: CERTIFICATE REQUEST**

1. In this phase we’ll create a new cert request from the Anchor server. Use the tool "DigiCertUtil.exe" under C:\Support on the Anchor server.
2. Run DigiCertUtil.exe. Click “I Accept” if prompted.
3. Go to "Create CSR" at the top right on the toolbar.
4. For Common Name, enter “cloud.<domain>.com”.
5. No Subject Alternative Names needed.
6. Under Organization, do a Network Solutions WHOIS search on the company’s name. Get the "Registrant Organization" value (this must be identical within the cert!).
7. For Department, enter "Information Technology".
8. City/State/Country fields must match the Registrant information from Network Solutions.
9. Click Generate.
10. Click "Save to file" to local C drive. This is the **private key**.
11. Go to Thawte Partner Center: <https://products.thawte.com/geocenter/reseller/logon.do>
12. Submit the cert request here.

(This is who we go through when we create these. A client may need us to go through a different registrar, e.g. GoDaddy.)

1. Select the number of years for which you’ll buy the new cert. The Business Office will provide it.
2. Request an SSL123 cert.
   1. Under Cert Signing Requirements, paste the private key text.
   2. Under Server Type, select “Microsoft IIS (All Versions).” Click Continue.
   3. Under Hashing Algorithm, select “SHA-256 with RSA and SHA-256 root.” Click Continue.
   4. Under Registration Information, verify that the information here matches the Network Solutions WHOIS information. If not, enter the correct values. Click Continue.
   5. Under Organizational Contact Information, enter the primary customer contact’s information. For Technical Contact, enter Robert’s information (if not already present). Click Continue.
   6. Select the Approval Email to send the cert approval to. Use a PlanetMagpie-accessible email address if at all possible. Otherwise, use the primary customer email listed. Click Continue.
   7. Click the options to agree with the submission agreements. Click Submit.
3. You (or the customer) will get an email from Thawte that you've submitted the request, titled, "SSL123 Certificate Order Confirmation". If the customer is emailed an approval request, request they forward it to you, in order for us to finalize the cert.
4. Click the link in the approval email. Afterward, you'll get another email saying "Your thawte SSL123 certificate is approved."
5. This email contains the cert details.
6. Save the cert code from “BEGIN CERTIFICATE” to “END CERTIFICATE”, as a .cer file in Notepad.
7. Copy it to the Anchor server, under C:\Support\CertificateRequests.
8. Launch DigiCert again. "Import" the .cer file.
9. Enter a new friendly name. Label it the name of the client, cloud.<domain>.com. Click Finish.
10. Highlight the cert, click Export Certificate. Choose "Key file (Apache compatible format)”. Save the key file.
11. Now you have **a .key file and a .crt file**.
12. Proceed to Phase 4.

**PHASE 4: CERTIFICATE IMPLEMENTATION**

Copy all .crt and private key files into E:\Apache24\conf\ssl.

**\*\*IMPORTANT:**  Make sure you’ve placed the files in the Apache24 subfolder, NOT the Apache2.2 subfolder! Make sure you’re working in the right folder.

Once in place, you’ll need to reference the SSL certificate location of those files in httpd.conf twice.

Part 1: Navigate to E:\Apache24\conf. Open httpd.conf in Notepad (as Administrator).

Scroll down in httpd.conf until you locate the last HTTP redirect snippet. It will look like this:

<VirtualHost 10.20.0.54:80>

    ServerName cloud.cbigproperties.com

    RewriteEngine On

    RewriteCond %{REQUEST\_URI} !^/updater

    RewriteCond %{REQUEST\_URI} !^/static/assets/

RewriteCond %{REQUEST\_URI} !^/server/hostname

    RewriteCond %{REQUEST\_URI} !^/static/assets/

    RewriteCond %{REQUEST\_URI} !^/server/hostname

    RewriteRule (.\*) <https://cloud.cbigproperties.com:510/auth/login?domain=corbo-brothers>

</VirtualHost>

Copy the most recent snippet & paste it below the </VirtualHost> line. You’ll modify this snippet to reference the new certificate.

1. Change the ServerName value to the value you entered in the new Anchor Organization’s settings (e.g., cloud.NewOrganization.com).
2. Change the RewriteRule value to match the new Anchor Organization. For the value after “domain=”, look in the new Anchor Organization’s settings, under Organization URL. Use the last value after “domain/” there.

Follow the same steps as above to change the IP and URL values.

Match the new .crt and .key filenames here as well.

Part 2: You must add the ServerName and reference the cert files in httpd.conf too. Scroll further down in httpd.conf until you locate the last snippet of this type:

<VirtualHost \_default\_:510>

SSLEngine on

ServerName cloud.cbigproperties.com

SSLCipherSuite ALL:!aNULL:!ADH:!eNULL:!LOW:!EXP:RC4+RSA:+HIGH:+MEDIUM

SSLCertificateFile "conf/ssl/cloud\_cbigproperties\_com.crt"

SSLCertificateKeyFile "conf/ssl/cloud\_cbigproperties\_com.key"

SSLCertificateChainFile "conf/ssl/CACert.crt"

AllowEncodedSlashes On

</VirtualHost>

Copy & paste the last entry. Then, modify it according to your new certificate filenames:

1. Change the local IP to the virtual IP set in Phase 1 (use 10.20.0.x, where x is 1 more than the last IP used).
2. Change ServerName to reflect the new customer’s domain.
3. Change the URLs for SSLCertificateFile and SSLCertificateKeyFile to match the new .crt and .key filenames you created.

Save httpd.conf when done. Close.

Navigate to the “E:\Data\Anchor Server\conf” subfolder.

Modify these two files in Notepad (as Administrator):

combined.key

all\_domain\_bundle.crt

Modifications for combined.key:

* Edit the file in Notepad.
* Append the private key of the domain you created. Copy all the contents of the domain's key file.
* Locate the last "---BEGIN CERTIFICATE---" in the file. This is the root certificate’s key. It MUST be the last certificate key listed in this file.
* Paste the domain’s key text **before** the root cert text in combined.key.
* Save and close.

Modifications for all\_domain\_bundle.crt:

* Edit the file in Notepad.
* Find the last "---BEGIN CERTIFICATE---" in the file. This is the root certificate. It MUST be the last certificate listed in this file.
* Copy the new domain's cert text, from “BEGIN CERTIFICATE” to “END CERTIFICATE”.
* Paste the text **before** the root cert text in all\_domain\_bundle.crt.
* Save and close.

[OPTIONAL] Once complete, you will need to make changes for the Mobile clients to work.

* Combine both the CA Root certificate and the SSL certificate as one .crt file. Do this by editing both .crt files in Notepad and creating one certificate file from them.
* Save as all\_domain\_bundle.crt in the E:\Anchor Server\conf folder.
* Copy the original private key request into this same folder.

Open Services.msc. Restart both the Apache 2.2 Service and the Anchor Server Service.

**\*\*Do this after hours to avoid disruption of existing customers’ Anchor clouds!**

NOTE: If the Apache service (on the server) doesn't start properly following these modifications, you have an issue in httpd.conf. If the Anchor Server service doesn't start properly, you have an issue in combined.key or all\_domain\_bundle.crt.

Test the new domain URL: cloud.<domain>.com. It should redirect to show “:510”, and display proper certificate identification (in the form of a lock icon on the address bar).

**PHASE 5: IMPORT USERS FROM ACTIVE DIRECTORY**

Importing users into Anchor from Active Directory is a two-step process:

1. Open port 389 on the LDAP server. (Bill/Robert)
2. Import the user accounts from Active Directory into Anchor.

\*\*Step 2 cannot be done without Step 1 completed first.

To complete Step 2:

1. Log into Anchor as an Organization Administrator.
2. Highlight the Organization box in the left column.
3. Click the arrow displayed on the box. Click Settings.
4. Click the Authentication button in the Settings window.
5. Click “Add Source”.
6. Under the Add Source window:
   1. Machine: Don’t use
   2. Host: Enter the IP of the Active Directory server/domain controller.
   3. Domain: Enter the company’s domain name.
   4. Login/Password: Use the domain’s administrative account. Email must be valid on the domain.
      1. If Anchor cannot access the appropriate server (Step 1), the Source will not be created.
7. Click Save.
8. Go into “Import Users”.
9. Under Organizational Unit, you should see “Active Directory”.
10. Select users to import by checking their checkboxes.
11. Click the Import Selected Users button.
12. “Welcome Email” and “WebDAV” are checked by default. Clear these checkboxes if requested, otherwise leave checked.

NOTE: If a user’s account name has changed, or they cannot access Anchor? Re-import the user with this process.

Designate a PlanetMagpie test user. If necessary, create a new user under Accounts.

Notify the user via email when it's created.

Using the username and password in the Welcome email, test the Anchor cloud setup. Log in & verify that the URL responds properly, the certificate displays correct security, and that Anchor files are accessible from outside the PlanetMagpie network.

**PHASE 6: FOLLOW-UP CHECKLIST**

* Ports 80, 443 and 510 opened in external DNS?
* Yes
* No
* Port 389 opened on the appropriate LDAP server (Robert/Bill to complete)?
* Yes
* No
* Firewall Setup in place? (Robert/Bill to complete)
* Yes
* No
* Logo Designed and Implemented in Custom Branding
* QuickCard Updated with Logo and URL
* Training Schedule Set

**DELETING A CUSTOMER’S ANCHOR FILESHARE**

If customer requests termination of service, there are 2 steps to follow for doing so: Making a full backup of the stored files, and deleting the Organization from Anchor.

1. Make a Full Backup of Stored Files

* If customer's Anchor files are less than 300GB, use an external hard drive. (If files are more than 300GB, use a direct server backup. Contact Larry for assistance.)
* Have a Systems Administrator log into the Anchor backend.
* Click the customer’s Organization.
* Click the Shares button. For each Team Share folder, click the Browse icon.
* You will see the Team Share's contents.
* Right-click each folder and select "Download ZIP." A ZIP file will download of the folder's contents.
* If there are loose files within the Team Share, right-click these files and select "Download."
* Once the Team Shares are downloaded, return to the Anchor backend.
* Click Accounts.
* For each customer account, click the Browse icon. Repeat the download process for each folder and any loose files.
* Save all resulting ZIP files to the external drive, in a folder marked with the customer name & backup date.

1. Delete the Customer’s Organization from Anchor  
   DO NOT DELETE THE ORGANIZATION UNTIL THE BACKUP IS COMPLETE!

* Click the customer’s Organization name in the left-hand column to select it.
* Click the Settings button.
* In the Organization Settings toolbar, you'll see the Delete Organization button (a trash can on the far right).
* Click the Delete Organization button.
* You will see a warning message. Click the Delete Organization button again.
* You will see a popup cautioning you that deleting an organization is irreversible. Click the Delete Organization button a final time.
* You will return to the Dashboard and should see a message confirming successful deletion.