Deploying Citrix Access Gateway VPX with Web Interface 5.4

Ben Piper
President
Ben Piper Consulting, LLC

Introduction

Deploying Citrix Access Gateway with Web Interface 5.4 is actually very easy, there are just some “gotchas” that you have to be ready for. This is a guide to help you avoid those snags and pitfalls that commonly occur with a Citrix Access Gateway VPX and Web Interface integration.

I recommend getting the Citrix Access Gateway VPX Getting Started Guide and HDX Remote Access Guide with Citrix Access Gateway VPX Express if you don’t already have them. The former document contains some inaccuracies but is has some useful reference info as well. The latter takes you through the fundamental setup of the Citrix Access Gateway VPX and gets you to the web administration console, where most of the meaty configuration will take place.

There are some assumptions made in this guide, including:

- The Citrix Access Gateway VPX has two virtual NICs, external to service external users, and internal for management and communication with the XenApp servers
- Two logon points will be configured: One that allows user authentication to take place at the web interface, and another that uses RADIUS
- The Citrix Access Gateway VPX will not reside in a DMZ. If your situation requires it to reside in a DMZ, setting it up is trivial once you’ve gotten everything else working.
- You’ve already got the Citrix Access Gateway VPX appliance imported and running, but not configured
- You have your web interface server setup, with no websites configured.
- You have installed the Citrix Access Gateway VPX license on a Citrix license server

Configuring Citrix Access Gateway VPX

Let’s get started! First, follow the Getting Started guide to configure the management interface for the Citrix Access Gateway via the VM console. If you are unsure about a setting, just take the default by hitting Enter.

Once you have your management IP assigned, you’ll need to access the web administration console by browsing to *https://[IP address]/lp/adminlogonpoint* . Login with the default username and password “admin”. You’ll see a nice dashboard with two dials and some nasty looking red X’s. Click on the Management tab. This will take you to the Networking portion of the System Administration menu group (Figure 1).

Here, enter the Citrix Access Gateway’s hostname as an FQDN. You’ll see a list of your network interfaces (eth0, eth1, etc.) with one of them having the management IP address you assigned. To the right, there are four checkboxes labelled Internal, External, Appliance Failover, and Management.

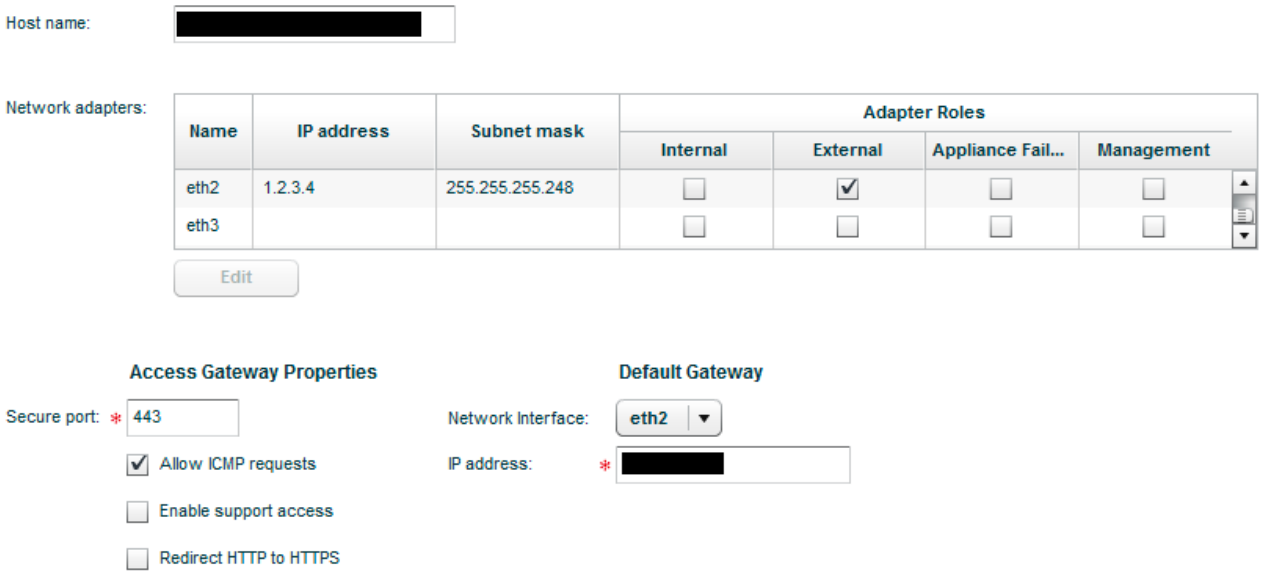

Figure 1

Moving from left to right, the interface that will be used to connect to your XenApp servers should have the Internal checkbox checked.

The interface for management should already have the Management checkbox checked.

The interface that will be receiving external requests from end users should have the External checkbox checked.

If need be, your Internal and External interfaces can be the same. Make sure your DNS servers have an entry for your Internal IP!

Under the Default Gateway section, select the interface the Citrix Access Gateway should use to route traffic for subnets to which it is not directly connected. This will probably be your External interface. Remember, the Citrix Access Gateway has a direct connection to the subnet your XenApp servers are on, so it doesn't need a gateway to get to those. But it does need a gateway to get back to your external users who are connecting from the Internet!

Click Save and restart the appliance using the big Restart button on the top right.

Log back into the web administration console and browse to Management > Name Server Providers (Figure 2). Enter your DNS servers and DNS suffixes.

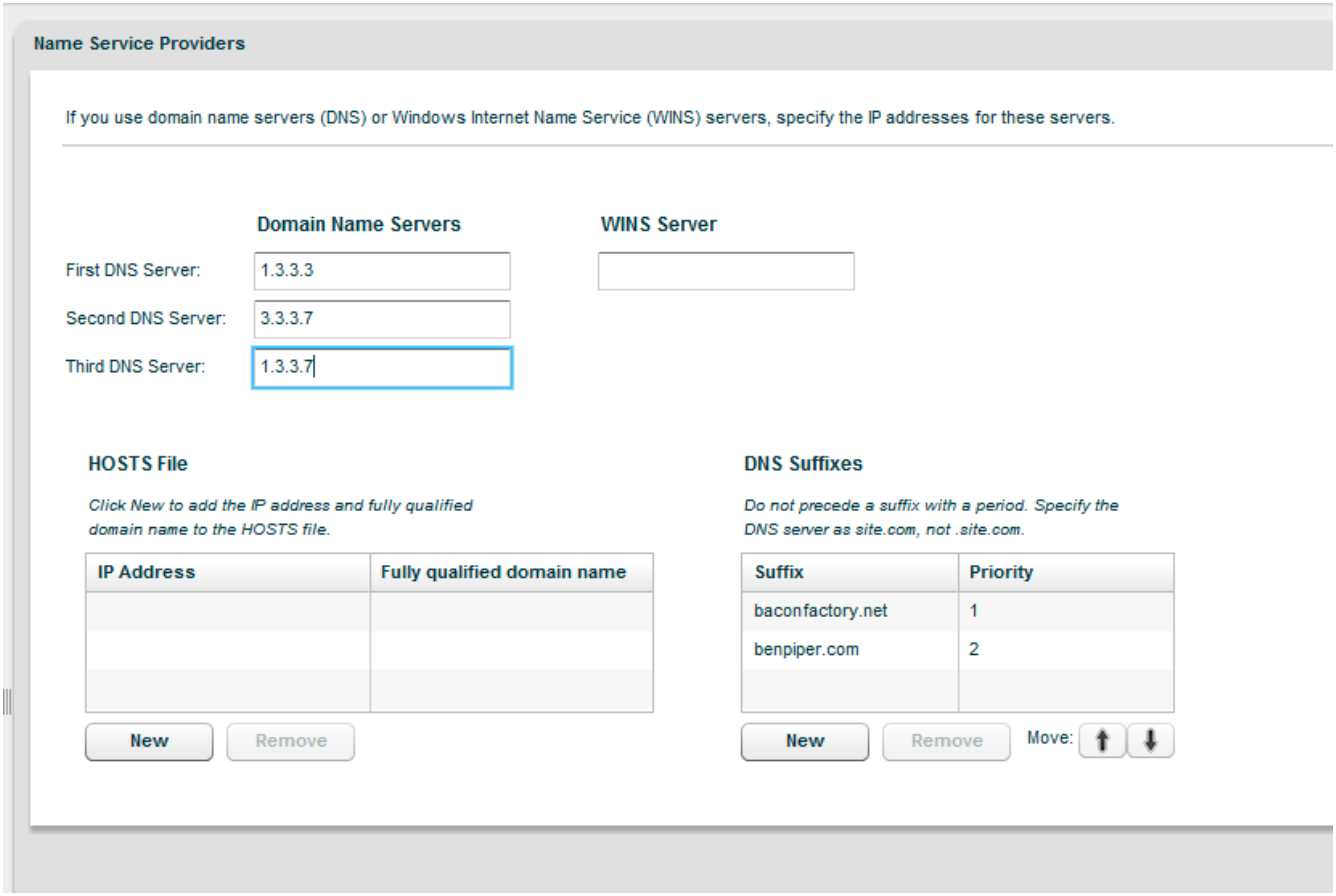

Figure 2

Now go to Static Routes in the System Administration menu. Do you need a static route? If you plan on putting the Citrix Access Gateway VPX into a DMZ later, go ahead and enter your static routes. Gateways you specify for static routes will take precedence over the default gateway you specified earlier. Remember, it does not hurt to add them now.

Now Browse down a few rows to Licensing and click Configure. Select the Licensing type and Remote Server for the licensing server. Enter the FQDN or IP of your Citrix licensing server, and click Save. The Citrix Access Gateway will attempt to grab its licenses and upon a successful retrieval, it will display them as shown in Figure 3:

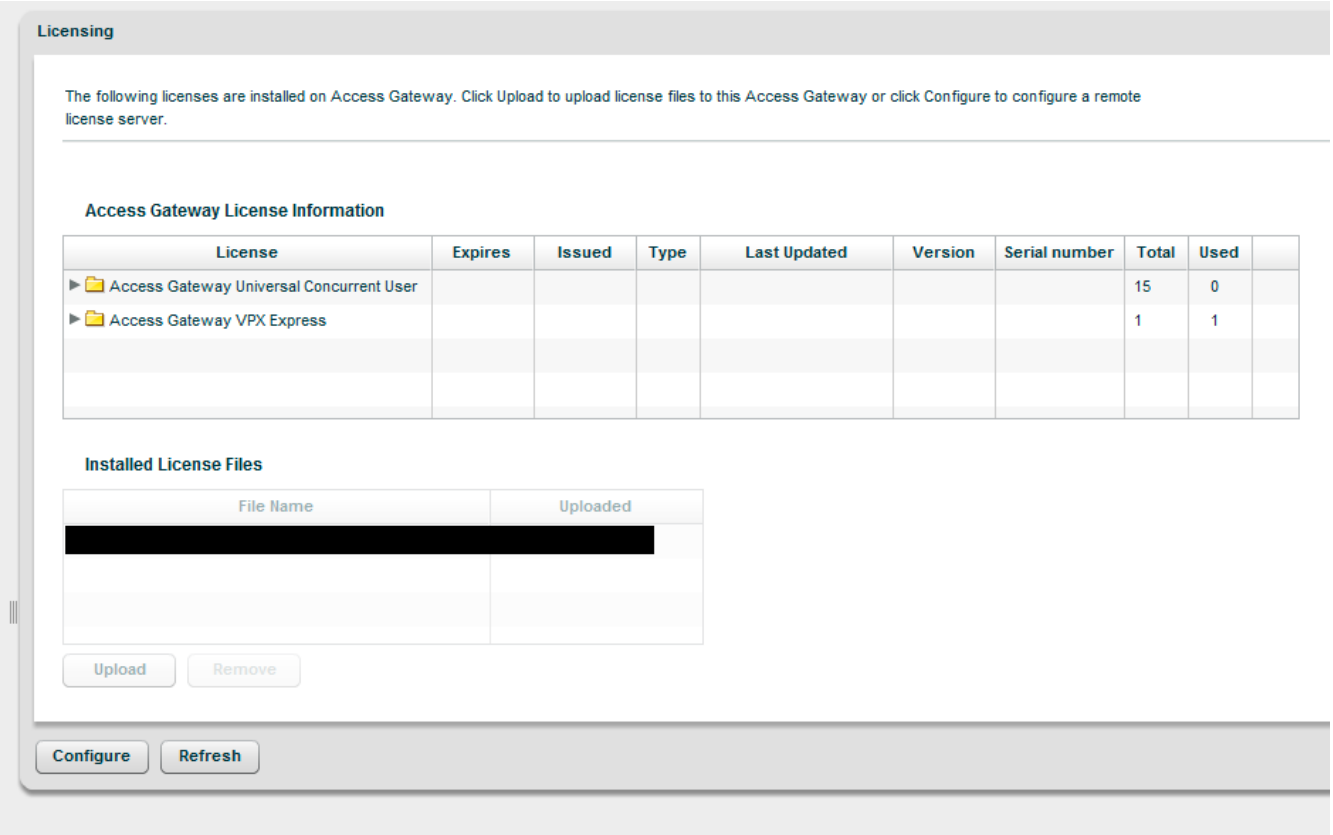

Figure 3

NB: If the Citrix Access Gateway is unable to retrieve the licenses, I recommend stopping and troubleshooting until it is able to successfully pick up the licenses. You can continue your configuration, but you will not be able to test it until the license issue is resolved.

Moving right along, click on Authentication Profiles under the Access Control menu group. It's time to add a RADIUS authentication profile! But before you do that, you have to set up a RADIUS server. I recommend reading How to Configure Radius Authentication/Authorization on Windows 2008 for Use on Citrix Access Gateway Standard Edition. (One caveat, however: don't perform steps 13-17 in the KB article because they're unnecessary and will cause problems.) Click Add and enter a name for the Authentication Profile. Click New and add your RADIUS server(s) and shared secret. Leave everything under Group Authorization as-is. You're relying on the RADIUS server to check group authorization.

Now go to XenApp or XenDesktop under Applications and Desktops and enter the IP ranges of clients that can access XenApp servers via ICA and CGP (Figure 4). I really don't know why there isn't a checkbox that allows you the equivalent of a "permit ip all", but there isn't.

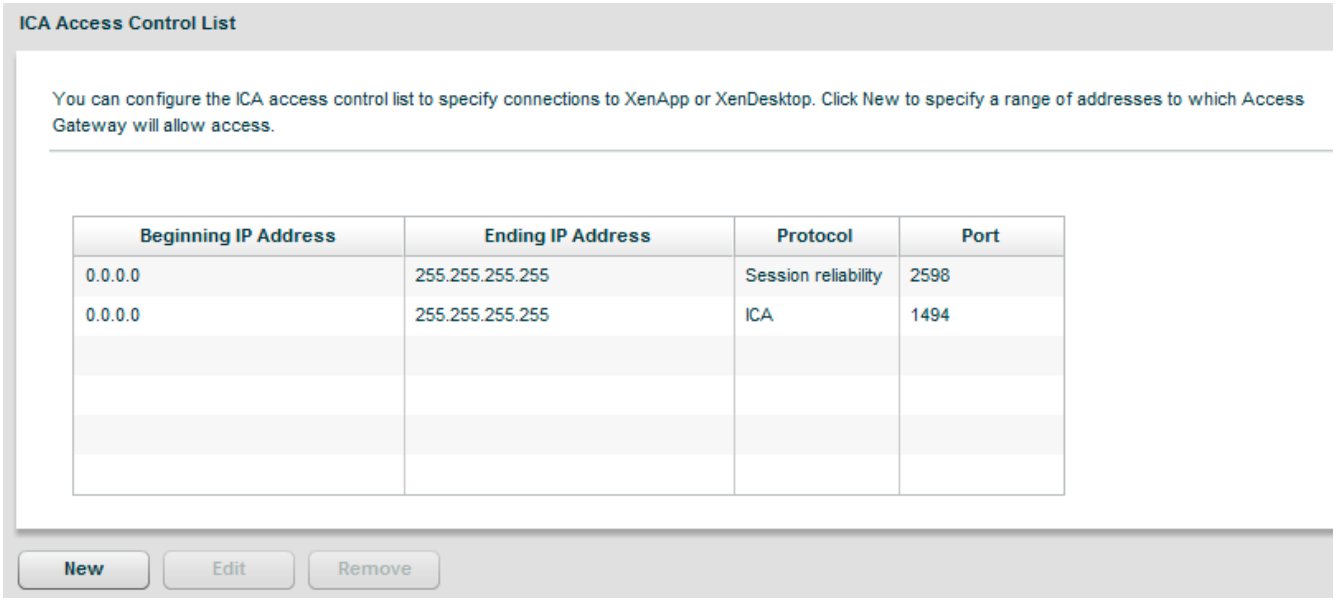

Figure 4

Next, click Secure Ticket Authority (Figure 5). These settings are arguably the most common cause of application launch issues. Select your STA servers carefully, and make sure all your XenApp servers have unique STA ID's! If you are running Provisioning Services and streaming XenApp, read How To Get a Unique STA ID for each of your Provisioned XenApp Servers before proceeding. Once you are sure your STA IDs are unique, click New and enter the FQDN of each XenApp server that will be providing STA services. By default, the connection type is Secure, but I'm guessing your XenApp servers are not using SSL for STA traffic, so select Unsecure. Leave everything else as-is and click Add. Note the servers you selected here, because you will need them later.

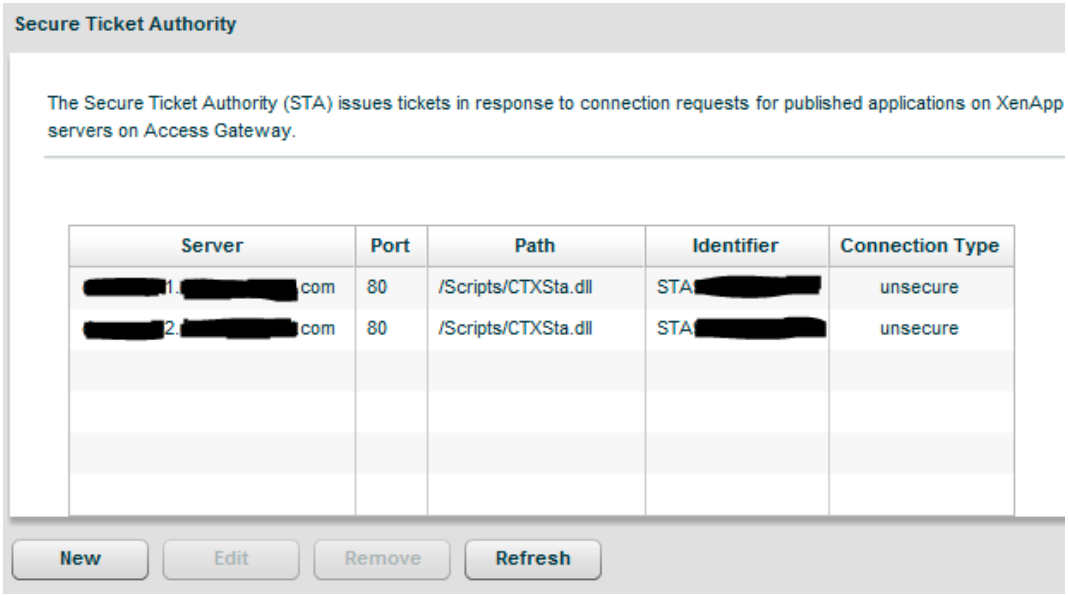

Figure 5

At this point you can go ahead and restart the Citrix Access Gateway VPX appliance, because it's now time to do some work on the Web Interface (WI) side.

Configuring Web Interface

Log into your WI server, launch the Citrix Web Interface Management console, and create a new site.

Should we do the easy one or the hard one first? Trick question. They're both easy! We'll set up a site to be used with RADIUS authentication. Click Create Site under the Actions pane on the right, name the website however you wish and click Next. Select "At Access Gateway" as the point of authentication and click Next (Figure 6). Here you'll be greeted with an intimidating looking Authentication Service URL field (Figure 7). But as I said, this is easy! Just enter *https://[cag-FQDN]/CitrixAuthService/AuthService.asmx* and click Next, Next. After a few moments, your site will be created.

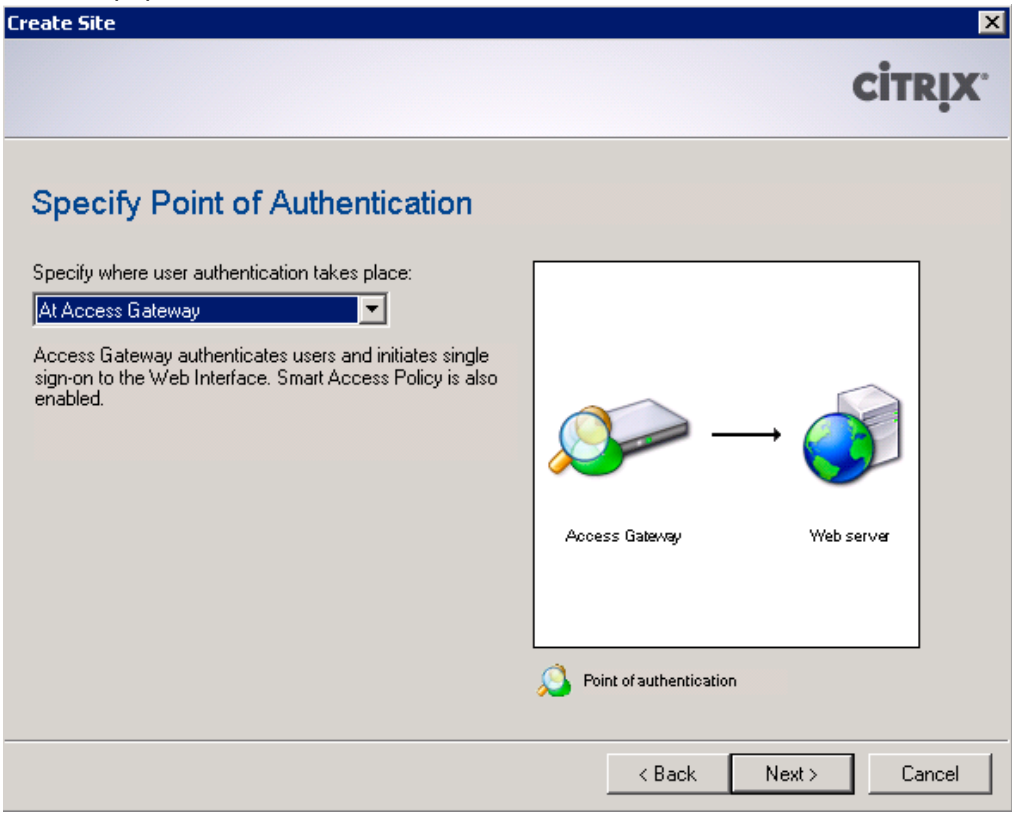

Figure 6

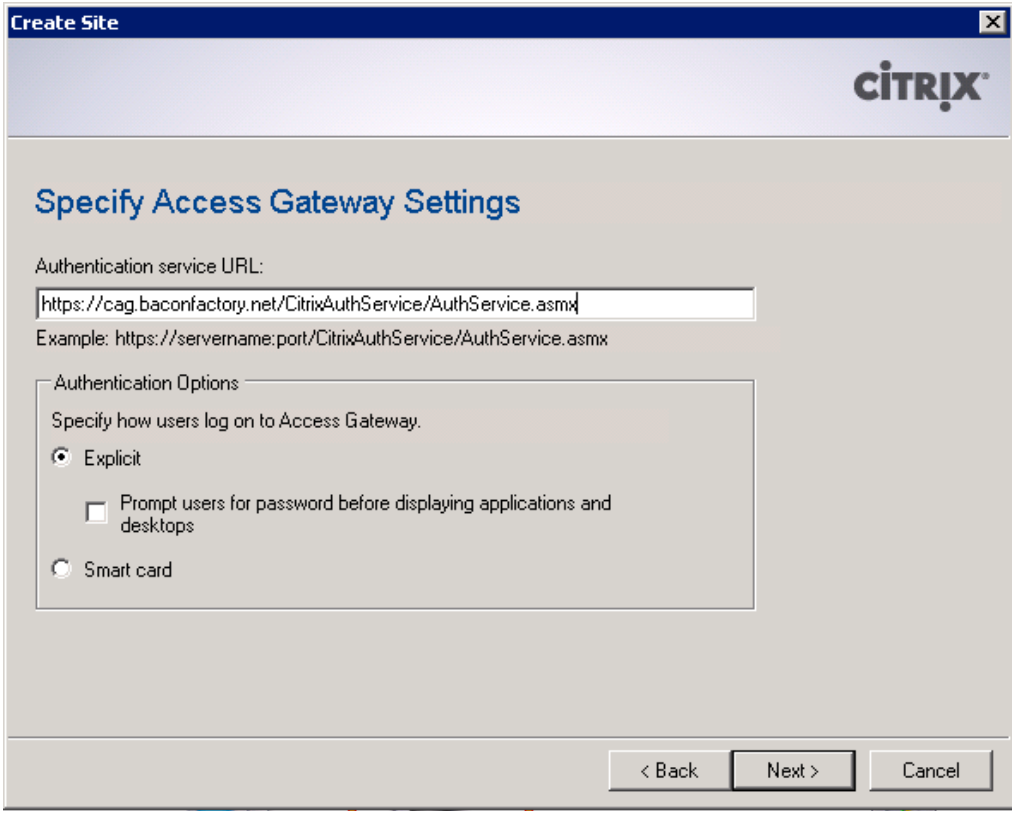

Figure 7

Right-click the site in the XenApp Web Sites list and select Server Farms. Configure your XenApp servers like you normally would in WI. There is nothing here unique to CAG.

Now right-click the site again and select Secure Access. Select the only item in the list and click Edit. Change Access method to Gateway direct and click Next. Next you'll be asked for the address of the Citrix Access Gateway (Figure 8). Enter the FQDN of the CAG, and optionally enable or disable session reliability. If enabled, you can request tickets from two STAs (A word on this option: When you setup a site for Citrix Receiver, this checkbox must be unchecked. This site you are creating now cannot be used for Receiver, so don't worry about it here if you plan to use Receiver.) Click Next.

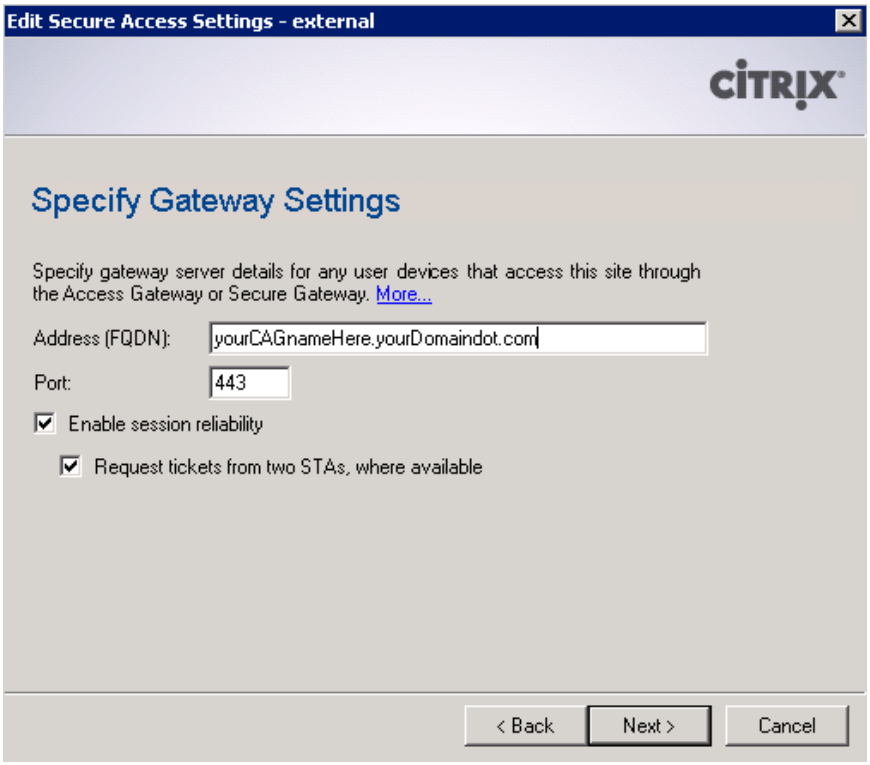

Figure 8

Remember I said to note the XenApp servers you entered into the CAG VPX as your STA servers? Web Interface wants to know about these servers too. Click Add and enter the URL of the first XenApp server you entered into the CAG in the following format (Figure 9):

http://xenapp1.baconfactory.net/scripts/ctxsta.dll

I still do not know why it doesn't just ask for the FQDN and assume the rest like the CAG does, but that's how it is. Do this for all STA servers you entered into the CAG, and in the same order. Check, double check, and triple check the URLs! Also optionally change the "Bypass failed servers for" option to 1 minute. Click Finish.

Figure 9

Are we done? Almost. The CAG should be back up now, so log back into it. Click Logon Points under Access Control and click New (Figure 10). Now don't be intimidated by all the settings. We only care about four things here. Enter the name of the logon point. Select this name carefully because it is what users will have to type in to connect to the CAG. If you enter "cag-logonpoint1" then users will have to go to *https://yourcag.yourdomain.com/lp/cag-logonpoint1* which just looks ugly! Under Type select Basic. In the Web Interface field, enter the URL of the web interface site you created (no trailing slash). Under Authentication Profiles, select the RADIUS authentication profile you created earlier. Finally, check the "Single sign-on to web interface" check box and click Save.

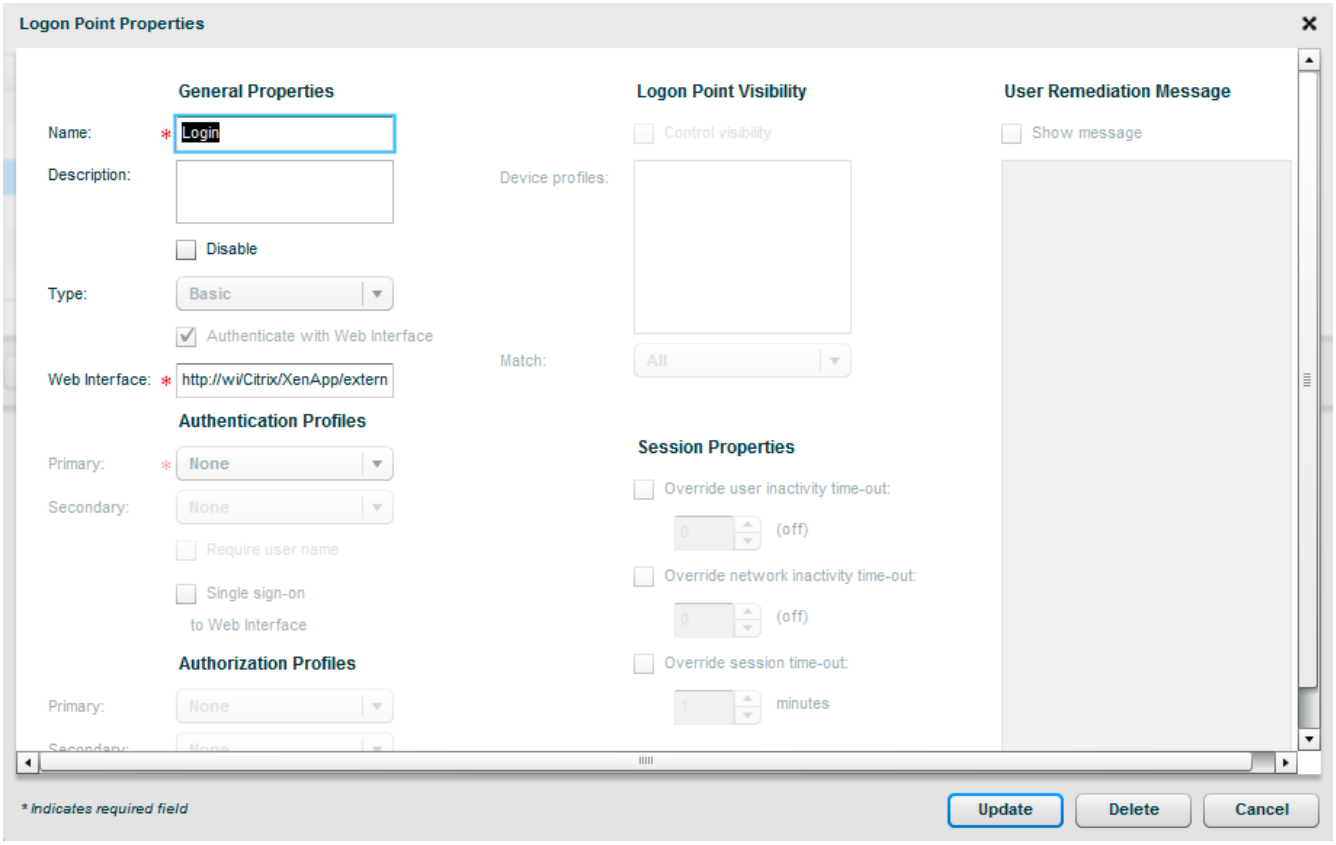

Figure 10

Now, we are almost ready to test. But to save ourselves from a disappointing moment of temporary CAG dysfunction, click on Secure Ticket Authority again. Do you see unique STA IDs populated next to each of your XenApp servers? If not, troubleshoot until you do. If so, it's time to test!

Browse to the logonpoint you just created. If you named your logonpoint "test1" and your CAG's FQDN is yourcag.yourdomain.com, browse to *https://yourcag.yourdomain.com/lp/test1*.

Do you get an SSL certificate error? Probably so. I intentionally did not cover installing a certificate because it introduces another level of complexity into the configuration. SSL Certificates are dependent on the FQDN, and the FQDN you use to connect to the CAG to enumerate and launch apps has to match up with the FQDN on the SSL certificate. The certificate also must be signed by a trusted certificate authority. Unless you have your own certificate authority, getting a signed certificate can be a pain. Unfortunately, connecting to CAGs using untrusted SSL certs causes a lot of problems. You may encounter some of these problems or you may not. Test anyway. If you do run into problems, the good news is that the heavy lifting of configuring the CAG is done.

Now, it's time for a moment of truth. Once you've gotten a login prompt, log in with an AD account that has appropriate authorization. You may need to specify the user in UPN or down-level domain format. It depends on your AD environment, but one of those should work. If you have trouble authenticating, first check the logs on the RADIUS server to make sure the denial is not occurring there. If you continue to have issues, it's time to get acquainted with what will become your new best friend: the CAG debug log. The CAG debug log is at your service at *https://yourcag.yourdomain.com/admin/d/?req=DebugLog* . Watch it for any FLEXnet or STA errors.

Once you get logged in, try launching a published app. If all goes well, you should see something like Figure 11.

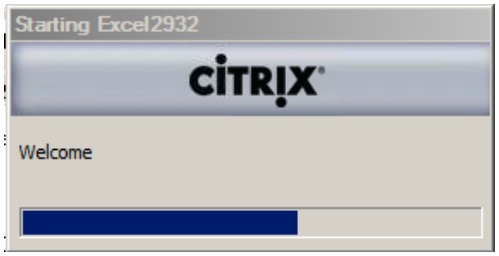

Figure 11

About Ben Piper

Ben Piper is the President of Ben Piper Consulting, LLC. *He can be reached at:*

12195 Alabama Road
Suite 114, Box 169
Woodstock, GA 30188

678-561-4236
ben@benpiper.com
Website: www.benpiper.com
Blog: blog.benpiper.com

