Contents

REQUIREMENTS .........................................................................................................................3
KNOWN LIMITATIONS ................................................................................................................3
TROUBLESHOOTING QUESTIONS TO ASK .............................................................................3
TROUBLESHOOTING TOOLS ....................................................................................................4
BASIC TROUBLESHOOTING GUIDELINES ..............................................................................5
SIMPLIFIED TRAFFIC FLOW:.....................................................................................................5
TROUBLESHOOTING SPECIFIC ISSUES ..................................................................................7

Invalid Server Certificate ...........................................................................................................7
Unable to load App List .............................................................................................................7

Connecting with Citrix Secure Gateway or directly to XenApp Services Site:.................................7
Connecting through Access Gateway Standard Edition ...............................................................7
Connecting through Access Gateway Advance Edition ...............................................................8
Connecting through Access Gateway Enterprise Edition ............................................................8

APPLICATION LAUNCH ISSUES ...............................................................................................8

Connecting Internally (No Gateway or Address Translations) ....................................................8
Connecting Externally with Access Gateway/Secure Gateway .....................................................9

Error 61 or Certificate is Untrusted ............................................................................................9

COMMON ERROR MESSAGES AND POSSIBLE CAUSES ....................................................10

Errors Enumerating Applications: ............................................................................................10
Errors When Launching Applications: .......................................................................................12

APPENDIX A ..............................................................................................................................14

Reading STA Logs ..................................................................................................................15

APPENDIX B – EXAMPLE OF IIS LOG ....................................................................................16

APPENDIX C - SAMPLE DEVICE CONFIGURATION SCREENS ..........................................17

iPhone/iPad: ............................................................................................................................17
Android: ......................................................................................................................................18

APPENDIX D - USING THE CHROME BROWSER TO VERIFY SESSION POLICY FOR
MOBILE DEVICES WITH ACCESS GATEWAY ENTERPRISE EDITION ................................20
Citrix Receiver for Mobile Devices Troubleshooting Guide

Product Home Page:


Requirements

- iPhone OS 2.2.1 or 3.x
- Presentation Server 4.5 or greater.
- A XenApp Services (Program Neighborhood Agent) Site configured. (Web Interface 5.x is required for external connections)

Known Limitations

- Session Reliability is not supported
- Does not support NetScaler self issued certificates
- When used with Citrix Secure Gateway, make sure “Use SSL” is checked in the XenApp Services Server configuration.
- Only works with Web Interface on IIS – does not work with Java Application Servers.

Troubleshooting Questions to Ask

- Are you connected to your network over wireless or are you using 3G?
- If using 3G, are you connected to your network through a VPN or are you going through Secure Gateway, Access Gateway Standard Edition, or Access Gateway Enterprise Edition? There must be a route to the Presentation Server from the iPhone on either the ICA port or through Secure Gateway / Access Gateway Enterprise Edition / Access Gateway Standard Edition.
- What is the address entered in Citrix Receiver? - Have you specified a path? If so what is it?
- A full path only needs to be entered if the Program Neighborhood Agent site is not the default site (/Citrix/Program Neighborhood Agent).
- Does it work with the Citrix Cloud Demo?
- What type of authentication are you using? Domain only, RSA + Domain, No Authentication?
- If using a Gateway Appliance is the appropriate type selected on the Mobile Device Settings?
Troubleshooting Tools

- Logfiles on the Citrix Access Gateway
- Logfiles on IIS
- STA Logging
- Event Viewer of Secure Gateway / Web Interface
- aaad.debug on Access Gateway Enterprise Edition
- Event Log Consolidator with Advanced Access Control
Basic Troubleshooting Guidelines

- Get the environment information.
- Understand the traffic flow.
- Identify where the connection is failing.

Simplified Traffic Flow:


Access Gateway Advance Edition
Access Gateway Standard Edition and Access Gateway Enterprise Edition have the same basic traffic flow – the Receiver connects to the Gateway and the requests are forwarded directly to the Web Interface server, then the Appliance relays the ICA traffic over port 1494 to the XenApp or XenDesktop servers.

With Advanced Access Control the traffic goes through an additional server – the Advanced Access Control server running on Windows 2003. The Web Interface server may also be on the Advanced Access Control server but may also be on another server.

When using Citrix Secure Gateway the connection can be configured several different ways. The important part to concentrate on is the IIS logs.

You can often identify where a connection is failing by watching the IIS logs. You should see several get and put requests from the CitrixReceiver from various devices (see Appendix for examples).

On Access Gateway Enterprise Edition, cat /tmp/aaad.debug to verify the device is hitting the Gateway and authenticating successfully. Verify session priority order, if you can see the authentication but do not see any connections from the CitrixReceiver in the IIS log.
Troubleshooting Specific Issues

Invalid Server Certificate

- What kind of SSL certificate is being used? A public Certificate Authority (CA) or an internal private Certificate Authority?
- If Private, is the CA certificate installed on the mobile device?
- Is there an intermediate certificate? Is it installed on the Gateway Server properly? (See Appendix for server specific instructions)

Unable to load App List

Connecting with Citrix Secure Gateway or directly to XenApp Services Site:

- Are any errors reported by the Receiver?
- Is the XenApp Services site in the default path? (/citrix/pnagent)
- What path if any is configured on the Receiver? (only needs to be the Server URL for default path, full path including the config.xml is required for custom paths, such as: /iPhone/config.xml)
- Is the address you are entering on the Receiver a public address or an internal IP address?
- Are there any errors in the event viewer of the Web Interface server?
- Make sure that "None" is selected for Access Gateway
- For use with Citrix Secure Gateway or with an IIS site secured with a certificate enter the URL as https://csg.company.com
- Do the IIS logs show a request from the Receiver?

Connecting through Access Gateway Standard Edition

- Are any errors reported by the Receiver?
- Is the XenApp Services site in the default path? (/citrix/pnagent)
- What path if any is configured on the Receiver? (only needs to be the Server URL for the default path, the full path including the config.xml is required for custom paths, such as: /iPhone/config.xml)
- Is Authentication being done at the Citrix Access Gateway?
- Are you using RSA Authentication + Active Directory?
- Is RSA the primary authorization type? (For two factor authentication, RSA must be primary, see the Administrator's guide)
- Do you see the requests from the Receiver in the IIS logs?
Connecting through Access Gateway Advance Edition

- If the logon point is named other than iPhone, make sure to enter the full path on the Receiver: https://aac.company.com/CitrixLogonPoint/logonpoint
- The Web Resource must be created as http://webintefaceserver/Citrix/PNAgent/ and published to the user as http://webintefaceserver/Citrix/PNAgent/config.xml
- Change the Home Page of the iPhone Logon Point to point to the Program Neighborhood Agent Web resource.
- Verify that, if you log on to this logon point from a web browser on the Advanced Access Control server itself, that the config.xml page is displayed without being prompted for anything else, such as client download or password notices.
- If there are any EPA Scans looking for operating system version, Anti-virus, and so on, create a filter so that they do not apply to the iPhone LogonPoint.
- Follow the logon through the Event Log Consolidator – it should stay on the iPhone logon point – if the session get sent back to the default logon point, something is denying access.

Connecting through Access Gateway Enterprise Edition

- Are any errors reported by the Receiver?
- Are you using two factor authentication?
- Is the Session Policy checking for the Receiver the highest priority?
- Do you see the request from the Receiver in the IIS logs?
- Are you using a self-signed certificate generated by the NetScaler? This is not supported at this time.

Application Launch Issues

The application list appears, but when they are launched, a black screen appears with "Please Wait" or no message.

After a period of time, the Receiver either closes or the user is taken back to the application list.

Reason: This often happens if the Receiver cannot connect to the XenApp Server or the Gateway Server.

Possible Causes:

Connecting Internally (No Gateway or Address Translations)

- iPhone is not connected to the internal wireless network but over the 3G network and there is no route to the XenApp Server
- DNS Resolution over XML is enabled on the Farm level and in Web Interface, and the iPhone is unable to resolve the FQDN of the XenApp server
Connecting Externally with Access Gateway/Secure Gateway

- Program Neighborhood Agent / XenApp Services site is not configured for Gateway Direct – Web Interface 4.x does not provide a method to configure Address Translation in the GUI.

- An invalid Gateway Address is entered in the Gateway Settings in the Access Management Console

- ICA Encryption is enabled on the application

- STA configured in Program Neighborhood Agent site is not in the Access Gateway / Secure Gateway STA List

- DNS Resolution over XML is enabled on the Farm level and in Web Interface and the Gateway is unable to resolve the FQDN of the XenApp server

- Server Certificate has an Intermediate Certificate that is not installed in the Local Computer Keystore of the Secure Gateway Server or on the Gateway Device

Error 61 or Certificate is Untrusted

- Verify the root certificate is installed on the iPhone, if it is a private certificate

- If there is an intermediate certificate involved, make sure the Intermediate is installed on the Gateway and linked to the Server Certificate on Access Gateway Enterprise Edition.
Common Error Messages and Possible Causes

Errors Enumerating Applications:

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Possible Cause / Resolution</th>
</tr>
</thead>
<tbody>
<tr>
<td><img src="image1" alt="Error Message" /></td>
<td>• The iPhone is unable to resolve the FQDN of the Gateway Server / XenApp Services Site. Test with Mobile Safari to verify it can resolve the FQDN.</td>
</tr>
<tr>
<td><img src="image2" alt="Error Message" /></td>
<td>• The certificate is untrusted. This might be caused by an intermediate certificate that is not linked properly on the Server.</td>
</tr>
</tbody>
</table>
• Verify that the proper version of Access Gateway is selected on the iPhone (Enterprise, Advanced or Standard).


• If using RSA Authentication + LDAP, make sure that RSA is the primary authentication type and that RSA is selected on the Receiver for iPhone.

• This might appear when using Access Gateway Enterprise Edition. Check the URL for the XenApp Services Site in the iPhone Session Profile and verify that it includes config.xml: For example: http://xenappservices/Citrix/PNAgent/config.xml

• This might also appear if accessing a Web Interface Site directly by HTTP when IIS is configured to only allow SSL connections.

• The Gateway Server might not be forwarding the request to the web server hosting the XenApp Services (Program Neighborhood Agent) site.

• Verify that the Gateway Device is passing the traffic to the Web server by checking the IIS logs on the Web server.

• If the traffic is making it to the Web server, check the event viewer, make sure there are no authentication errors or issues connecting to the XML service.
Errors When Launching Applications:

<table>
<thead>
<tr>
<th>Error Message</th>
<th>Possible Case</th>
</tr>
</thead>
<tbody>
<tr>
<td>When attempting to launch the application, this message appears. Check the Event Viewer on the Web Interface server for errors – this can be caused by an invalid STA, server too busy, errors of type IMA.</td>
<td>• This can be similar to the error “There was an error connecting to the requested resource” with Web Interface.</td>
</tr>
<tr>
<td>• This can be similar to the error “There was an error connecting to the requested resource” with Web Interface.</td>
<td>• Might occur when connecting through Citrix Secure Gateway.</td>
</tr>
<tr>
<td>• Might occur when connecting through Citrix Secure Gateway.</td>
<td>• Can be caused by the same problems as ‘Untrusted Certificate’:</td>
</tr>
<tr>
<td>• Can be caused by the same problems as ‘Untrusted Certificate’:</td>
<td>o Intermediate Not Installed on Server</td>
</tr>
<tr>
<td>• Can be caused by the same problems as ‘Untrusted Certificate’:</td>
<td>o Private Root Certificate</td>
</tr>
</tbody>
</table>
These might all be caused the same thing - connection between one of the components in a Citrix Access Gateway / Secure Gateway connection has failed.

- Connection from client to Gateway
- No licenses on the Gateway
- Untrusted STA – verify STA list in the Program Neighborhood Agent site matches the list in the Gateway
- Route from Gateway to XenApp Server – verify port 1494 is open to each XenApp Server

See Appendix A
Appendix A

SSL Error - Proxy Denied Access / No SSL Server at Requested Address

- Error 4
- Error 21
- Error 23
- Error 29
- Error 37

These can all be caused the same thing - connection between one of the components in a Citrix Access Gateway / Secure Gateway connection has failed.


Troubleshooting:

- Verify client can connect to the Citrix Access Gateway by FQDN and not just by IP address
- Verify the Citrix Access Gateway has licenses installed and allocated
- Verify that the STA list matches in the Web Interface and Citrix Access Gateway / Secure Gateway
  Important Web Interface 5.x defaults to DNS-Port which do not work with ICA ACLs
- Verify that ports 1494 and 2598 are open between the Gateway and each XenApp server hosting applications.

If the STA ID and connection are verified, the issue could be a problem between the Citrix Access Gateway and the XenApp server.

In the XenApp Services/Program Neighborhood Agent configuration, remove all but one STA.

Change the logging level on the STA to 3 by modifying the CTXSta.config file in the appropriate directory.

Restart the XML service (iisreset if sharing with IIS).

Reproduce the issue.

Reading STA Logs

For every successful connection, there should be two entries in the STA Log (three if Session Reliability is enabled).

Request Ticket Successful - this is the Web Interface requesting the ticket for the launched application.
Request Data Successful - this is the Citrix Access Gateway validating the ticket provided by the client.

If you receive both of these messages, verify that the Citrix Access Gateway can connect to the Presentation Server that is listed in the STA Ticket (see STA Logs to see what to look for).

If the XenApp Server is listed in the STA Log by IP Address, do a port scan from the Citrix Access Gateway Admin Desktop by IP address, if it is shown as the FQDN, do the scan by FQDN. From Access Gateway Enterprise Edition, do a telnet from the CLI.
Reading STA Logs

For every successful connection, there should be two entries in the STA Log (three if Session Reliability is enabled).

Request Ticket Successful - this is the Web Interface requesting the ticket for the launched application.
Request Data Successful - this is the Citrix Access Gateway validating the ticket provided by the client.

An STA Ticket includes the following information - Ticket Number (Randomly generated one time use hash), Address of the XenApp Server, Username and Domain, and the Application that was launched and the Protocol type. If Enable DNS over XML is enabled on the XenApp Server Farm level and Web Interface AddressResolutionType is set to DNS-Port (default with Web Interface 5.x), then the FQDN of the XenApp server appears instead of the IP Address (see the Session Reliability examples).

A normal connection without session reliability:

Web Interface Requests Ticket:
INFORMATION 2009/03/16:14:17:07 CSG1305 Request Ticket - Successful. 9FD7DC64C6CB7D60311F7CB4A4765 V1 10.54.74.148:1494 <xml version="1.0"?><ctxConnInfoProtocol SYSTEM "CtxConnInfo.dtd"><ctxConnInfo version="1.0"><serverAddress>10.54.74.148:1494</serverAddress><username>scott</username><userDomain>dragons</userDomain><ApplicationName>SSL Relay Notepad</ApplicationName><Protocol>ICA</Protocol></ctxConnInfo>

Secure Gateway Validates the Ticket:
INFORMATION 2009/03/16:14:17:10 CSG1304 Request Data - Successful. 9FD7DC64C6CB7D60311F7CB4A4765 V1 10.54.74.148:1494 <xml version="1.0"?><ctxConnInfoProtocol SYSTEM "CtxConnInfo.dtd"><ctxConnInfo version="1.0"><serverAddress>10.54.74.148:1494</serverAddress><username>scott</username><userDomain>dragons</userDomain><ApplicationName>SSL Relay Notepad</ApplicationName><Protocol>ICA</Protocol></ctxConnInfo>

When Session Reliability is enabled, the ticket contains CGP information - you also get a second ticket request for each connection:

INFORMATION 2009/03/17:15:17:14 CSG1305 Request Ticket - Successful. 3C117C4BA9F3CB3DF7BBB5740634599 V4 CGPAddress = atl3scottm64.dragons.citrix.com:2598:localhost:1494 Refreshable = false XData = <xml version="1.0"?><ctxConnInfoProtocol SYSTEM "CtxConnInfo.dtd"><ctxConnInfo version="1.0"><serverAddress>atl3scottm64.dragons.citrix.com:1494</serverAddress><username>scott</username><userDomain>dragons</userDomain><ApplicationName>SSL Relay Notepad</ApplicationName><Protocol>ICA</Protocol></ctxConnInfo>

INFORMATION 2009/03/17:15:17:17 CSG1304 Request Data - Successful. 3C117C4BA9F3CB3DF7BBB5740634599 V4 CGPAddress = atl3scottm64.dragons.citrix.com:2598:localhost:1494 Refreshable = false XData = <xml version="1.0"?><ctxConnInfoProtocol SYSTEM "CtxConnInfo.dtd"><ctxConnInfo version="1.0"><serverAddress>atl3scottm64.dragons.citrix.com:1494</serverAddress><username>scott</username><userDomain>dragons</userDomain><ApplicationName>SSL Relay Notepad</ApplicationName><Protocol>ICA</Protocol></ctxConnInfo>

INFORMATION 2009/03/17:15:17:17 CSG1305 Request Ticket - Successful. F78ABF0B5FE9D45D9F5881E64211E2C4 V4 Refreshable XData = <xml version="1.0"?><ctxConnInfoProtocol SYSTEM "CtxConnInfo.dtd"><ctxConnInfo version="1.0"><serverAddress>atl3scottm64.dragons.citrix.com:1494</serverAddress><username>scott</username><userDomain>dragons</userDomain><ApplicationName>SSL Relay Notepad</ApplicationName><Protocol>ICA</Protocol></ctxConnInfo>

SSLRelayAddress = atl3scottm64.dragons.citrix.com:443 ICAAddress
Appendix B – Example of IIS Log

The IIS logs shows the User Agent as CitrixReceiver, the platform and the version of the Receiver being used.

Example of a successful enumeration and launch from a Gateway Appliance with an IP Address of 10.54.72.151 using the receiver for iPhone:

2009-07-06 13:59:49 W3SVC1 10.54.74.160 GET /Citrix/pnagent/config.xml - 80 - 10.54.72.151 CitrixReceiver/2.3+CFNetwork/445.6+Darwin/10.0.0d3 200 0 0

2009-07-06 14:00:31 W3SVC1 10.54.74.160 POST /Citrix/pnagent/enum.aspx - 80 - 10.54.72.151 CitrixReceiver/2.3+CFNetwork/445.6+Darwin/10.0.0d3 200 0 0

2009-07-06 14:02:11 W3SVC1 10.54.74.160 POST /Citrix/pnagent/launch.aspx - 80 - 10.54.72.151 CitrixReceiver/2.3+CFNetwork/445.6+Darwin/10.0.0d3 200 0 0

iPad:

2010-03-30 15:29:13 W3SVC1 10.54.74.160 GET /Citrix/PNAgent/config.xml - 80 - 10.54.74.160 - 200 0 0
2010-03-30 15:33:10 W3SVC1 10.54.74.160 POST /Citrix/PNAgent/enum.aspx - 80 - 10.54.74.204 CitrixReceiver-iPad/1.0+CFNetwork/467.12+Darwin/10.2.0 200 0 0
2010-03-30 15:33:29 W3SVC1 10.54.74.160 POST /Citrix/PNAgent/launch.aspx - 80 - 10.54.74.204 CitrixReceiver-iPad/1.0+CFNetwork/467.12+Darwin/10.2.0 200 0 0

Android:

2010-04-02 22:47:03 W3SVC1 10.54.74.160 GET /citrix/pnagent/config.xml - 80 - 10.54.74.200 CitrixReceiver/1.0.1029+Android/2.1 200 0 0
2010-04-02 22:47:10 W3SVC1 10.54.74.160 POST /citrix/pnagent/enum.aspx - 80 - 10.54.74.200 CitrixReceiver/1.0.1029+Android/2.1 200 0 0
2010-04-02 22:57:14 W3SVC1 10.54.74.160 POST /citrix/pnagent/launch.aspx - 80 - 10.54.74.200 CitrixReceiver/1.0.1029+Android/2.1 200 0 0
Appendix C - Sample Device Configuration Screens

iPhone/iPad:

<table>
<thead>
<tr>
<th>Citrix Secure Gateway</th>
<th>Gateway Options</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Citrix Secure Gateway access, enter HTTPS and the FQDN, if you are not accessing using HTTPS, just use the FQDN or IP address.</td>
<td>When using an Access Gateway, enter the FQDN of the Access Gateway, you do not need to add HTTPS. Check the Use Citrix Access Gateway box, then select the Gateway type and proper authentication type.</td>
</tr>
</tbody>
</table>
Android:

<table>
<thead>
<tr>
<th>Citrix Secure Gateway / Direct to Program Neighborhood Agent</th>
<th>Gateway Settings</th>
</tr>
</thead>
<tbody>
<tr>
<td>For Citrix Secure Gateway access, enter HTTPS and the FQDN, if you are not accessing using HTTPS, just use the FQDN or IP address.</td>
<td>When using an Access Gateway, enter the FQDN of the Access Gateway, you do not need to add HTTPS. Check the Use Citrix Access Gateway box, then select the Gateway type and proper authentication type.</td>
</tr>
</tbody>
</table>

![Gateway Type](image1.png)

- Standard Edition
- Advanced Edition
- Enterprise Edition

![Gateway Authentication](image2.png)

- No Authentication
- Domain Only
- RSA SecurID© Only
- Domain + RSA SecurID©
Appendix D - Using the Chrome Browser to Verify Session Policy for Mobile Devices with Access Gateway Enterprise Edition

When using the Receiver for Mobile Devices with Access Gateway Enterprise Edition, it can be difficult to determine what is occurring if the Receiver is not enumerating applications properly.

When checking the IIS logs, if you do not see any entries from the CitrixReceiver, you can verify your session policy for the Mobile Devices by adding a header check for a non standard browser, such as Chrome from Google.

In your Access Gateway Session Policy, add a condition such as this:

REQ.HTTP.HEADER.User-Agent CONTAINS Chrome

Make sure that “Match Any Expression” is selected. This applies the policy for the Receiver for Mobile Devices to the Chrome browser as well.

Using the Chrome Browser, log on to your Access Gateway Enterprise Edition normally. You should get taken directly to the config.xml page. If you are not, any error messages or prompts should assist in debugging connection problems or configuration issues.