Checklist for troubleshooting Outlook connectivity in Exchange 2013 and 2016 (on-premises)

[The Exchange Team](https://social.technet.microsoft.com/profile/The+Exchange+Team)May 31, 2016[10](https://blogs.technet.microsoft.com/exchange/2016/05/31/checklist-for-troubleshooting-outlook-connectivity-in-exchange-2013-and-2016-on-premises/#comments)

Initial published link:

<https://blogs.technet.microsoft.com/exchange/2016/05/31/checklist-for-troubleshooting-outlook-connectivity-in-exchange-2013-and-2016-on-premises/>

Some of relatively common and difficult issues we see in support are related to Outlook connectivity to Exchange.  There are several variations that we classify as connectivity (related to server performance or otherwise).  They can include:

* Clients prompting for credentials (intermittently or continuously)
* Clients getting disconnected
* Clients are unable to establish a connection
* Clients freezing or going unresponsive

There are many factors that can contribute to these symptoms, and each one can lead down a completely different troubleshooting path. In this particular post we will focus on methods and tools to troubleshoot these. There are too many potential underlying causes to cover them all but hopefully this will serve as a good starting point for troubleshooting.

This post is not meant to be a post that you necessarily read from start to finish, but rather serve as a guidance for when you need to troubleshoot hard to find issues related to client connectivity. It can be a bit overwhelming, sure, but depending on the depth that you need to get into – it might be all worth it!

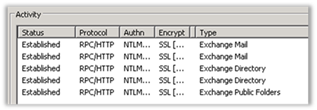
Note: If you are an Office 365 customer with users having mailboxes in Exchange Online, we highly recommend using our new **Office 365 Support and Recovery Assistant** (aka **SaRA**) to troubleshoot Outlook connectivity and other common issues. SaRA is available at [http://diagnostics.office.com](http://diagnostics.office.com/).

In every case, it's best to spend some time understanding what the user is actually experiencing. Understanding the full client experience and effect can help determine the logging and troubleshooting path. When you define the users issue, you should also run the **Microsoft Office Configuration Analyzer Tool (**[**OffCAT**](https://www.microsoft.com/en-us/download/details.aspx?id=36852)**)**on the client to have a good view of configuration that can impact their experience.

Client configuration

Here are some examples of things to consider when troubleshooting these issues.

* Are the clients connecting with Outlook Anywhere or MAPI/HTTP? Try to use the Outlook “Connection Status” window to access more information on the user’s connection by holding down the CTRL key and clicking the Outlook icon in the system tray so that the “Connection Status” window appears. Here you can see the protocol, the connection type, and so on RPC/HTTP indicates Outlook Anywhere, whereas HTTP indicates MAPI/HTTP.

[](https://msdnshared.blob.core.windows.net/media/2016/05/image939.png)

* Are clients online or in cached mode? Cached mode is recommended. Moving critical users to cached mode to improve their experience might be a good thing. You can enable BitLocker if there are local storage considerations. What devices are clients traversing to hit the CAS? Run Tracert to the CAS to determine the devices in the path of the client.
* Test several clients with a hosts file pointing to the IP address of CAS using the external host name. The Hosts file is located in C:\Windows\System32\Drivers\etc directory.
* What is the user attempting to do when they experience issues? Accessing a calendar, public folders or just moving around in the Inbox?
* Are effected mailboxes on the same database, same server?
* What is the Outlook full build number? Always make sure that you are working with an updated client. Information about recent updates can be found in the following references:
  + [How to install the latest applicable updates for Microsoft Outlook](http://support.microsoft.com/en-us/kb/2625547/en-us)
  + [Outlook and Outlook for Mac Update File Versions](http://social.technet.microsoft.com/wiki/contents/articles/31133.outlook-and-outlook-for-mac-update-build-numbers.aspx)
* Using the OffCAT output, examine which add-ins are being used and consider disabling those for testing. Make sure that you restart Outlook and verify the add-ins remain disabled.
* Try running Outlook in safe mode for a few clients. Not all add-ins are removed when using safe mode so ensure you have verified they are no longer loaded with [Process Explorer](https://technet.microsoft.com/en-us/sysinternals/bb896653) if you suspect they are still loaded.
* Enable Outlook logging.

CAS configuration

The first step for the Exchange server checks is to review all the settings noted in TechNet article, [Exchange 2013 Sizing and Configuration Recommendations](https://technet.microsoft.com/en-us/library/dn879075(v=exchg.150).aspx). Several items such as setting power management to “High Performance” and verify the OS isn't turning off power to the NIC. Making sure the server is running updated and supported .NET version, and so on are extremely important:

* Run the [Exchange Performance Health Checker](https://gallery.technet.microsoft.com/Exchange-2013-Performance-23bcca58) script. Review the output for any results that have to be updated.
* As of right now, Exchange 2013 should be running .NET 4.5.2. Please see the [Supportability Matrix](https://technet.microsoft.com/en-us/library/ff728623(v=exchg.150).aspx) for current version supported.
* [Turn off hyper-threading](http://blogs.technet.com/b/exchange/archive/2015/09/15/ask-the-perf-guy-what-s-the-story-with-hyperthreading-and-virtualization.aspx)
* [Update outdated Outlook clients](https://support.microsoft.com/en-us/kb/2625547)
* Update NIC drivers
* Eliminate any slow disk issues identified in Perfmon
* Set Power Management to “High Performance”
* Locate the NIC “Properties |Configure | Power Management” and verify the box for “[Allow the computer to turn off this device to save power](http://blogs.technet.com/b/exchange/archive/2013/10/22/do-you-have-a-sleepy-nic.aspx)” is unchecked.
* Verify [RSS and Chimney offload on CAS](http://blogs.technet.com/b/exchange/archive/2013/07/30/a-reminder-on-real-life-performance-impact-of-windows-snp-features.aspx).
* Verify that all the noted hotfixes are installed from [Exchange 2013 Sizing and Configuration Recommendations](https://technet.microsoft.com/en-us/library/dn879075(v=exchg.150).aspx).
* CAS Keep Alive values should be set to 30 minutes and no less than 15 minutes. If there's no entry in the registry for KeepAliveTime then the value is 2 hours. This value, if not set correctly, can affect both connectivity and performance as noted in KB, [Unable to connect using Exchange ActiveSync due to Exchange resource consumption](https://support.microsoft.com/en-us/kb/2469722). You must make sure that the load balancer and any other devices in the path from client to CAS be set correctly. More information on load balancer settings are listed later in this document under Load Balancing Configuration section. The goal is to set CAS with the lowest value so that client sessions when ended, are ended by the CAS and not by a device.

Path: HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Tcpip\Parameters\  
Value name: KeepAliveTime  
Value Type: 1800000 (30 minutes, in milliseconds) (Decimal)

* Max Core Count - In Exchange 2013 and 2016, you can encounter performance problems if you go too far off of the preferred architecture, particularly when referring to core count. This can even include having too many cores. The maximum number of cores on a server should be no more than 24. Hyper-threading can artificially inflate this value so it's important to disable it as mentioned. For more information, refer to following articles:
  + [Troubleshooting High CPU utilization issues in Exchange 2013](http://blogs.technet.com/b/exchange/archive/2015/04/30/troubleshooting-high-cpu-utilization-issues-in-exchange-2013.aspx)
  + [Ask the Perf Guy: How big is too BIG?](http://blogs.technet.com/b/exchange/archive/2015/06/19/ask-the-perf-guy-how-big-is-too-big.aspx)
* As a general statement, [Preferred Architecture](http://blogs.technet.com/b/exchange/archive/2014/04/21/the-preferred-architecture.aspx) should be your guidance.

Load balancer configuration

Please note that for 3rd party load balancer configuration, you should always refer to product documentation / guidance. The following are some general best practices and things we see misconfigured:

1. Verify the client TCP Idle Time-Out is a slightly larger value than the Keep Alive setting on CAS, as noted earlier.

In this example, we are using the 30-minute Keep Alive on CAS and we have both a firewall and load balancer in front of the clients. Here is the connection path.

Clients > Firewall > Load Balancer > CAS

In this example, if you have a firewall in the path from client to CAS, we are referencing the firewall “idle” time out and not the persistence time out. This value should be greater than the load balancer and the load balancer time out should be greater than CAS. Note that it is not recommended to go below 15 minutes for Keep Alive on CAS or TCP idle timeout on the load balancer.

Firewall time out = 40 minutes  
LB TCP Idle time out = 35 minutes  
CAS Keep Alive = 30 minutes

2. If the load balancer supports it, the preferred option is to configure it to use “Least Connections” with “Slow start” during typical operation.

*With the “least connections” method, be mindful it is possible for a CAS to become overloaded and unresponsive during a CAS outage or during patching/maintenance. In the context of Exchange performance, authentication is an expensive operation.*

The TechNet article [Exchange 2013 Sizing and Configuration Recommendations](https://technet.microsoft.com/en-us/library/dn879075(v=exchg.150).aspx) describes the differences as:

*A hardware or software load balancer should be used to manage all inbound traffic to Client Access servers. The selection of the target server can be determined with methods such as “round-robin,” in which each inbound connection goes to the next target server in a circular list, or with “least connections,” in which the load balancer sends each new connection to the server that has the fewest established connections at that time. These methods are detailed further in the following blog*[*Load Balancing in Exchange 2013*](http://blogs.technet.com/b/exchange/archive/2014/03/05/load-balancing-in-exchange-2013.aspx)*and TechNet*[*Load balancing*](https://technet.microsoft.com/en-us/library/jj898588(v=exchg.150).aspx)*.*

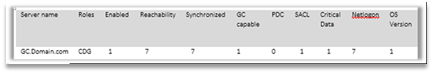
3. For ActiveSync persistence setting, set the load balancer to use “Authorization header cookie" to avoid one CAS becoming overloaded because source IP will send all the connections to one server as [per this](https://blogs.technet.microsoft.com/mikehall/2012/09/05/why-the-correct-load-balancing-persistence-is-so-important-in-exchange-server-2010/).

Additional troubleshooting steps

If you have completed the previous steps and you are still experiencing issues, the following data is necessary:

* Start Perfwiz on CAS and Mailbox server to run for 4 hours during the busiest part of the day (assuming this is when issues are happening). Download ExPerfwiz from [here](http://experfwiz.codeplex.com/). Example command line: *\experfwiz.ps1 -server MBXServer -interval 10 -filepath D:\Logs.*Once you have the performance data, see blog on [Troubleshooting High CPU Utilization issues in Exchange 2013](http://blogs.technet.com/b/exchange/archive/2015/04/30/troubleshooting-high-cpu-utilization-issues-in-exchange-2013.aspx)
* Review the application logs for any 4999 events that occurred around the time of problems.
* In the Application log, review the 2080 event to make sure that all domain controllers are responding with correct Boolean values. If there are any responses that are not accurate, the DC’s should be repaired or excluded.

Expected values are“**CDG 1 7 7 1 0 1 1 7 1**” as shown in the following table.

[](https://msdnshared.blob.core.windows.net/media/2016/05/image940.png)

For testing, a DC can be excluded by using the Set-Exchangeserver –StaticExcludedDomainControllers parameter as shown in this section, however, troubleshooting [Global Catalog access](https://support.microsoft.com/en-us/kb/298879) should also be done as soon as your testing is completed. Statically excluding a GC takes effect immediately and will be viewable on the next 2080 Event ID with all zero values. Some additional resources on the subject:

* + - [The PDC column should show 0 and not be used by Exchange](https://support.microsoft.com/en-us/kb/298879)
    - More information for Set-ExchangeServer is located [here](http://technet.microsoft.com/en-us/library/bb123716.aspx)
    - More information about Event ID 2080 from MSExchangeDSAccess can be found [here](http://support.microsoft.com/kb/316300/EN-US)

* When in Application log, also check for Event ID 2070 or 2095. A 2070 event occurs when Exchange tries to query a DC and fails and it cannot contact/communicate with a DC. If this event occurs during the time when clients have issues (or frequently), then it should be investigated. If you only see this event occasionally over several days, it could be a result of the DC being restarted during maintenance. The same is true with event 2095; infrequent isn't a concern but continued logging of this event could be a sign of a problem.
* Always ensure MaxConcurrentApi bottlenecks are not present in the environment. To avoid this problem now or in future review the following information:
  + [You are intermittently prompted for credentials or experience time-outs when you connect to Authenticated Services](http://support.microsoft.com/kb/975363)
  + [Updated - NTLM and MCA Concerns](http://blogs.technet.com/b/ad/archive/2008/09/23/ntlm-and-maxconcurrentapi-concerns.aspx)
  + [Quick Reference: Troubleshooting, Diagnosing, and Tuning MaxConcurrentApi Issues](https://blogs.technet.microsoft.com/askpfeplat/2014/01/12/quick-reference-troubleshooting-diagnosing-and-tuning-maxconcurrentapi-issues/)
* LDAP latencies can impact server and client performance. When you work with client connectivity issues, the LDAP counter can help point delays with communications to the DC’s. These are under the *MSExchange ADAccess Domain Controllers(\*) LDAP Read Time* and *LDAP Search Time*, and is recommended that the average be within 50ms and spikes no greater than 100ms. More information [here](http://blogs.technet.com/b/askpfeplat/archive/2015/05/11/how-to-find-expensive-inefficient-and-long-running-ldap-queries-in-active-directory.aspx).

Coexistence with Exchange 2010 and 2007

In order to coexist with newer versions of Exchange, certain configuration steps are necessary. This section outlines typical organization changes that are needed to connect through an Exchange 2013 CAS.

* Verify that legacy servers are at the latest available Service Pack and RU.
* If Outlook Anywhere is not enabled on legacy Exchange servers, we recommend that you enable Outlook Anywhere on every CAS in the organization with NTLM authentication for ClientAuthenticationMethod and NTLM and Basic for IISAuthenticationMethods. The external host name should be the DNS name of the Exchange 2013 CAS external URL.

Example:  
Enable-OutlookAnywhere -Server 'ConE10' -ExternalHostname Mail.Contoso.com' -ClientAuthenticationMethod 'Ntlm' -SSLOffloading $false –IISAuthenticationMethod Basic, NTLM

* Configure the Exchange 2010 SCP for AutoDiscover to point to Exchange 2013 CAS. The AutoDiscover SCP is used for the internal clients only. In some cases, you can just update DNS to point to Exchange 2013. DNS would have to point AutoDiscover to Exchange 2013 for all the external clients also. We do not recommend that you use separate URL’s for legacy mailboxes. All connections should use an Exchange 2013 CAS.

To set the SCP for AutoDiscover (example):  
Set-ClientAccessServer ConE10 -AutoDiscoverServiceInternalUri [https://Mail.Contoso.com/autodiscover/autodiscover.xml](https://mail.contoso.com/autodiscover/autodiscover.xml)

* Verify all legacy CAS are pointed to 2013 for the SCP AutoDiscover URI.

Example:  
Get-ClientAccessServer |fl \*uri\*  
AutoDiscoverServiceInternalUri : [https://Mail.Contoso.com/autodiscover/autodiscover.xml](https://mail.contoso.com/autodiscover/autodiscover.xml)

* Be aware that Exchange 2007 mailboxes will access EWS and OAB by using “Legacy.Domain.com” as discussed [here](http://blogs.technet.com/b/exchange/archive/2014/03/12/client-connectivity-in-an-exchange-2013-coexistence-environment.aspx).

Known issues in coexistence

* [Mailboxes located on 2010 Unable to Connect through Exchange 2013](https://support.microsoft.com/en-us/kb/2990117)
* Users may be prompted for credentials when accessing additional mailboxes, calendars or Public Folders on Exchange 2010 server. See #2 in the previous section indicating that NTLM is not enabled on legacy CAS for Outlook Anywhere.

Troubleshooting Logs and Tools

***HTTP Proxy RPCHTTP Logs***

In Exchange 2013, there are several logs in the logging folder. For Outlook clients one of the first logs to examine are the HTTP Proxy logs on CAS. The connection walk-through section shows the process that is used to connect to Exchange 2013. This complete process is logged in the HTTP Proxy log. Also, if it is possible, add Hosts file to the client for one specific CAS to reduce the number of logs.

The logs on CAS are located here by default: *C:\Program Files\Microsoft\Exchange Server\V15\Logging\HttpProxy\RpcHttp*

***HTTP Proxy AutoDiscover Logs***

Exchange 2013 has HTTP Proxy logs for AutoDiscover that are similar to the logs shown earlier that can be used to determine whether AutoDiscover is failing.

The logs on CAS are located here by default: *C:\Program Files\Microsoft\Exchange Server\V15\Logging\HttpProxy\AutoDiscover*

***HTTP Error Logs***

HTTP Error logs are failures that occur with HTTP.SYS before hitting IIS. However, not all errors for connections to web sites and app pools are seen in the httperr log. For example, if ASP.NET threw the error it may not be logged in the HTTP Error log. By default, HTTP error logs are located in *C:\Windows\System32\LogFiles\HTTPERR*. Information on the httperr log and codes can be found [here](https://support.microsoft.com/en-us/kb/820729/).

***IIS Logs***

IIS logs can be used to review the connection for RPC/HTTP, MAPI/HTTP, EWS, OAB, and AutoDiscover. The full data for the MAPI/HTTP and RPC/HTTP is not always put in the IIS logs. Therefore, there is a possibility that the 200 connection successful may not be seen. [IIS codes](https://support.microsoft.com/en-us/kb/943891).

In Exchange 2013 IIS logs on the CAS should contain all user connections on port 443. IIS logs on the Mailbox server should only contain connections from the CAS server on port 444.

Most HTTP connections are first sent anonymously which results in a 401 challenge response. This response includes the authentication types available in the response header. The client should then try to connect again by using one of these authentication methods. Therefore, a 401 status found inside an IIS log does not necessarily indicate an error.

Note that an anonymous request is expected to show a 401 response. You can identify anonymous requests because the domain\username is not listed in the request.

***RPC Client Access (RCA) Logs***

The RCA logs can be used to find when a user has made a connection to their mailbox, or a connection to an alternate mailbox, errors that occur with the connection, and more information. RCA logs are located in the logging directory which is located at *%ExchangeInstallPath%\Logging\RpcClientAccess*. By default, these logs have a maximum size of 10MB and roll over when size limit is reached or at the end of the day (based on GMT), and the server keeps 1GB in the log directory.

***Outlook ETL Logging (requires a support case with Microsoft to analyze the log)***

ETL logs are located in %temp%/Outlook Logging and are named Outlook-#####.ETL. The numbers are randomly generated by the system.

To enable Outlook logging

In the Outlook interface:

* Open Outlook.
* Click **File**, **Options**, **Advanced**.
* Enable “Enable troubleshooting logging (requires restarting Outlook)”
* Restart Outlook.

How to enable Outlook logging in the registry:

* Browse to HKEY\_CURRENT\_USER\Software\Microsoft\Office\xx.0\Outlook\Options\Mail
* DWORD: EnableLogging
* Value: 1
* Note: xx.0 is a placeholder for your version of Office. 15.0 = Office 2013, 14.0 = Office 2010

***ExPerfwiz (Perfmon for Exchange)***

You can use Perfmon for issues that you suspect are caused by performance. <http://experfwiz.codeplex.com/>

Exchange 2013 has daily performance logs that captures the majority of what is needed. These logs are by default located in C:\Program Files\Microsoft\Exchange Server\V15\Logging\Diagnostics\DailyPerformanceLogs

***Log Parser Studio***

[Log Parser Studio](https://gallery.technet.microsoft.com/office/Log-Parser-Studio-cd458765) is a GUI for Log Parser 2.2. LPS greatly reduces complexity when parsing logs. Additionally, it can parse many kinds of logs including IIS Logs, HTTPErr Logs, Event Logs (both live and EVT/EVTX/CSV), all Exchange protocol logs from 2003-2013, any text based logs, CSV logs and ExTRA traces that were converted to CSV logs. LPS can parse many GB of logs concurrently (we have tested with total log sizes of >60GB).

Blog with tips/how to about LPS: <http://blogs.technet.com/b/karywa/>

***Exmon tool (aka Microsoft Exchange Server User Monitor)***

We use [this tool](http://blogs.technet.com/b/exchange/archive/2016/02/16/exchange-2013-and-2016-exmon-tool-is-now-available.aspx) to get detailed information about client traffic.

Hopefully this is helpful; we expect that we will make some updates to this checklist as time goes on!

Thanks to Brendon Lee, Marc Nivens, Nasir Ali, Louise Budrow and [The Exchange Performance V-Team](http://aka.ms/exchangeperf) for technical review.

Charlene Weber