DOWNLOAD PDF LOGGING DEVICE ERRORS

Chapter 1 : Exchange ActiveSync Mailbox Logging â€“ Jason Slaughter

Drivers, like most Microsoft Windows system components, can log errors to the system event log. The errors are visible in the Event Viewer. This section includes the following topics.

Records the operational health of the certificate registration point. Certificate registration point Records details about the installation and configuration of the certificate registration point. Certificate registration point Records challenge verification and certificate enrollment activities. For example, look for messages from the NetworkDeviceEnrollmentService source. You can also use the following log files: Client notification The following table lists the log files that contain information related to client notification. Log name Computer with log file bgbmgr. Also records information about the generation of online and task status files to be sent to the site server. Management point Records the activities of the notification server installation wrapper process during installation and uninstallation. Management point Records details about the notification server installation and uninstallation. Client Cloud management gateway The following table lists the log files that contain information related to the cloud management gateway. Log name Computer with log file CloudMgr. The component functionality is merged into the CMG service component. The cloud management gateway pushes logs to Azure storage every five minutes. So the maximum delay is 10 minutes. Verbose switches affect both local and remote logs. The actual file names include the service name and role instance identifier. Compliance settings and company resource access The following table lists the log files that contain information related to compliance settings and company resource access. Log name Computer with log file CIAgent. Client Records information about configuration item task scheduling. Client Records high-level information about the evaluation, conflict reporting, and remediation of configuration items and applications. Client Records information about reporting policy platform results into state messages for configuration items. Client Records information about reading configuration item synclets from WMI. Client The following table lists the log files that contain information related to conditional access.

Chapter 2 : Troubleshooting Exchange ActiveSync and reading IIS logs Â« calendrierdelascience.com

Check engine gauges and the LED of the device to make sure that the vehicle is compatible with the device. Two blinks on the LED indicates that the device is not able to establish communications with the vehicle.

The development of the Semantic Web and the Internet of Things is likely to accelerate this present trend. Instrumentation protocols[edit] Several protocols have been standardised including a smart protocol, SDI , that allows some instrumentation to be connected to a variety of data loggers. The use of this standard has not gained much acceptance outside the environmental industry. SDI also supports multi drop instruments. This has been used traditionally in the industrial control area, and there are many industrial instruments which support this communication standard. Some data loggers use a flexible scripting environment to adapt themselves to various non-standard protocols. Data logging versus data acquisition[edit] The terms data logging and data acquisition are often used interchangeably. However, in a historical context they are quite different. A data logger is a data acquisition system, but a data acquisition system is not necessarily a data logger. Data loggers typically have slower sample rates. A maximum sample rate of 1 Hz may be considered to be very fast for a data logger, yet very slow for a typical data acquisition system. Data loggers are implicitly stand-alone devices, while typical data acquisition system must remain tethered to a computer to acquire data. This stand-alone aspect of data loggers implies on-board memory that is used to store acquired data. Sometimes this memory is very large to accommodate many days, or even months, of unattended recording. Earlier data loggers used magnetic tape , punched paper tape, or directly viewable records such as "strip chart recorders ". Given the extended recording times of data loggers, they typically feature a mechanism to record the date and time in a timestamp to ensure that each recorded data value is associated with a date and time of acquisition in order to produce a sequence of events. As such, data loggers typically employ built-in real-time clocks whose published drift can be an important consideration when choosing between data loggers. Data loggers range from simple single-channel input to complex multi-channel instruments. Typically, the simpler the device the less programming flexibility. Some more sophisticated instruments allow for cross-channel computations and alarms based on predetermined conditions. The newest of data loggers can serve web pages, allowing numerous people to monitor a system remotely. The unattended and remote nature of many data logger applications implies the need in some applications to operate from a DC power source, such as a battery. Solar power may be used to supplement these power sources. These constraints have generally led to ensure that the devices they market are extremely power efficient relative to computers. In many cases they are required to operate in harsh environmental conditions where computers will not function reliably. Portable Dataloggers may reach up to 20 channels with maximum 10ms Hz sampling rate. This unattended nature also dictates that data loggers must be extremely reliable. Since they may operate for long periods nonstop with little or no human supervision, and may be installed in harsh or remote locations, it is imperative that so long as they have power, they will not fail to log data for any reason. Manufacturers go to great length to ensure that the devices can be depended on in these applications. As such dataloggers are almost completely immune to the problems that might affect a general-purpose computer in the same application, such as program crashes and the instability of some operating systems. Unattended hydrographic recording such as water level, water depth, water flow, water pH, water conductivity. Unattended soil moisture level recording. Unattended gas pressure recording. Offshore buoys for recording a variety of environmental conditions. Measure temperatures humidity, etc. Process monitoring for maintenance and troubleshooting applications. Process monitoring to verify warranty conditions Measure vibration and handling shock drop height environment of distribution packaging.

Chapter 3 : Log files for troubleshooting - Configuration Manager | Microsoft Docs

The question is, How can one design a logging subsystem that can log these kinds of errors? Event if it's enough to issue one DMA request to write to HDD, no paging, no interrupts, it's still at lot of work to do on a presumably failed hardware.

Messages that are matched by the event list named event-list defined in Step 2 are forwarded to the logging destination. NOTE You might find it confusing that logging messages sent as SNMP traps are configured using logging history and messages sent as Syslog packets are configured using logging trap. Unfortunately, the term "trap" has a different meaning here. Optional Identify the firewall in Syslog messages: However, you can define one unique identifier for your firewall that also appears in the text of each Syslog message. For example, the following firewall is named InnerSanctum. It identifies itself using its host name: Firewall config hostname InnerSanctum Firewall config logging device-id hostname Identify a Syslog server destination: By default, messages are sent using UDP port Obviously, the Syslog server must be configured to listen on the matching protocol and port number. The firewall in the following example sends its trap logging messages to the Syslog server using the default UDP port Firewall config logging host inside NOTE Keep in mind that the firewall sends a copy of each Syslog message generated to each of the configured Syslog servers. If your firewall is heavily utilized and is configured to generate high-severity messages to multiple Syslog servers, its performance can be affected. Normally, Syslog messages are sent using UDP port This provides an easy way to send messages in a best-effort fashion. The firewall has no idea if the messages are being received by the Syslog server, much less if there is actually a Syslog server at the address. Some environments require strict collection of security information. In this case, you should use TCP to send Syslog messages, usually over port The firewall opens a TCP connection with the Syslog server. As long as the connection is open, the firewall is certain that the messages are being reliably received. In fact, the TCP Syslog method is designed to be so reliable that the connection closes if the Syslog server becomes unavailable or if its logging storage becomes full. At this point, the firewall immediately stops forwarding traffic and generates a " The PIX is disallowing new connections" message. You can also see this with the show logging command, as in the following example. Firewall show logging Syslog logging: Firewall config logging permit-hostdown Optional Tune the Syslog transmission queue. As Syslog messages are generated, they are placed in a queue for transmission. If messages are being generated faster than they can be sent, the logging queue begins to fill. By default, a firewall queues up to messages. As soon as this threshold is reached, any new messages are simply dropped and are not sent. You can see information about the logging queue with the following EXEC command: Firewall show logging queue The output from this command displays the size of the queue, along with the current queue depth and the high-water mark. If the msgs most on queue value is , the queue filled up at some point, and messages have been lost. In the following example, a high volume of logging messages is being generated, but they are being transmitted fast enough that the queue has never filled. Firewall show logging queue Logging Queue length limit: Use the following configuration command: You can use the show blocks EXEC command to see how much memory is available before tuning the queue. Syslog messages use byte blocks of memory. Be careful not to allocate too much of this memory to the logging queue, because the byte blocks are also used for stateful failover message queuing. Optional Add time stamps to Syslog messages: Firewall config logging timestamp By default, Syslog messages are sent with no indication of the date or time at which they occurred. In this case, the Syslog server should add its own time stamps to the messages as they are received. Make sure the Syslog server synchronizes its clock with a known and accurate source. The logging timestamp command causes the firewall to add a time stamp to each Syslog message before it is sent. The firewall should have its clock set and time synchronized to a known and accurate sourceâ€”preferably an NTP server that is common to all devices on your network. TIP If the logging timestamp command is used to make the firewall add time stamps, it is also possible that the Syslog server is configured to add its own time stamps. This can result in logging messages that have double time stamps in the text. Many Syslog servers can be configured to detect this and strip the extra time stamp automatically. Optional Set the Syslog facility:

DOWNLOAD PDF LOGGING DEVICE ERRORS

Firewall config logging facility facility Syslog servers can collect logging messages from a variety of sources. Messages are marked with a facility number 0 to 23 , allowing the Syslog server to classify and store messages from similar sources. The default facility, 20, is also known as the Local4 facility. This is usually expected by most Syslog server implementations. Optional Generate Syslog messages from the standby failover unit: If your environment needs strict collection of logging information, you can use this command to cause the standby firewall to generate Syslog messages too. The standby firewall can generate the same Syslog messages as the active unit only because the same state information is passed from the active unit to the passive unit. This doubles the number of messages sent to the Syslog server s , and each message is duplicated. However, if the active unit fails, any messages that were queued might be lost. The standby unit continues sending those messages as if nothing happened. Optional Log to an e-mail address. When logging messages are generated, they can be sent to an e-mail address. Each message is sent as a single e-mail message. You can configure the "From" and "To" addresses for the resulting e-mails. The firewall always sends these with the subject line "PIX Alert hostname. Tue, 3 May Inbound TCP connection denied from Set the mail logging level:

Chapter 4 : usb - Which Windows 7 log file contains device connection/disconnection information? - Super

In the list of devices, select the device that you want to track, and then click Start Logging. In the Information dialog box, click Yes. Reproduce the behavior that you want to capture, and then click Retrieve Log.

Although people are now moving towards Gmail yet many people just love and use Yahoo email services. People also face problems with Yahoo email login screen. Whenever I login to Yahoo account using my laptop, it works fine but sometimes on my mobile phone, I get login errors similar to this one: Please sign in from our desktop log in screen and then try login again from our mobile login screen. So, here I found a simple solution of Yahoo email login error. Actually the problem is with the URL used to access Yahoo email login page. In order to sign in to Yahoo mail from mobile devices, you will have to follow the URL given below: Account credentials and check your Yahoo email from mobile devices without login errors. Actually the problem is with the mobile login page of Yahoo email. So, that solves the Yahoo email login problem. Yahoo Email Login Page Redirection Issue Another issue that is being faced by many Yahoo users is that after logging in to Yahoo email account, it redirects back to the Yahoo email login page. This problem is caused if you are currently logged into any other Yahoo account. So, it is recommended that you should sign out from Yahoo and clear your browser cookies and cache. Again login to Yahoo Email and you will see everything working smoothly. Also provides alternative email login options to their users. You can sign in to Yahoo email account by connecting your Facebook account with Yahoo. For linking Yahoo account with Facebook, you will have to authorize Yahoo application for Facebook to access your account details. It will also require your Yahoo account password for the first time. After successful connection, you will be able to log in to Yahoo mail by using Facebook account. With the popularity of Google Gmail among internet users, Yahoo also listed Google as the alternative login for Yahoo email. You can use your Google account to access Yahoo email by linking both accounts. So, if you forget your Yahoo email password, still you can access Yahoo email by using Google account. Quick Links Yahoo Account Recovery You can easily reset password of Yahoo email or recover it using alternate email address or mobile phone verification. It is recommended that you should use Yahoo mobile apps for accessing Yahoo email using mobile phones. Follow the links below to get Yahoo mail mobile apps.

Chapter 5 : syslog - Wikipedia

Simply log into ECP and go to Options -> Phone -> Mobile Phones/Devices. This slab contains a list of the EAS devices for the mailbox, and users can enable logging and retrieve it from here. The log will be sent to the user's mailbox.

PCIe provides two mechanisms for error handling. Base line error handling mechanism. The PCIe baseline error handling mechanism can also be categorized as below: Supports the software or devices that have no knowledge of PCIe. Supports the software or devices that have knowledge of PCIe. Advanced error reporting mechanism. Error logging using PCI-compatible registers: These errors are mapped within PCI compatible error registers. Error logging using PCIe capability registers: This method is error reporting of PCIe native devices. This is optional method where error reporting is done by the registers which are mapped into the extended configuration address space. PCI-Compatible or legacy error handling mechanism: The PCI Express mechanisms for handling these events are via the split transaction mechanism transaction completions and virtual SERR signaling via error messages. This involves enabling error reporting and setting status bits that can be read by PCI-compliant software. There is the configuration status and command registers, which have error related bits. Below are the details of some important registers required for PCI compatible error handling. Error messages are sent by the device that has detected either a fatal or non-fatal error. Note that reporting in some cases is device-specific. This provides the bits to indicate the type of error such as system error, target abort. These registers include error detection and handling bit fields regarding the nature of an error that is supplied with standard PCI error handling. The baseline capability register space is different for RC and EP mode. PCIe Baseline capability registers structure These registers provide support for: Setting the corresponding bit in the device control register enables the generation of the corresponding error message which reports errors associated with each classification. An error status bit is set any time an error associated with its classification is detected. These bits are set irrespective of the setting of the error reporting enable bits within the device control register. Because Unsupported Request errors are by default considered Non-Fatal Errors, when these errors occur both the Non-Fatal Error status bit and the Unsupported Request status bit will be set. Note that these bits are cleared by software when writing a one 1 to the bit field. Link control and link status register The physical link connecting two devices may fail causing a variety of errors. Link failures are typically detected within the physical layer and communicated to the Data Link Layer. Because the link has incurred errors, the error cannot be reported to the host via the failed link. Therefore, link errors must be reported via the upstream port of switches or by the Root Port itself. Also the related fields in the PCI Express Link Control and Status registers are only valid in Switch and Root downstream ports never within endpoint devices or switch upstream ports. This permits system software to access link-related error registers on the port that is closest to the host. AER provides the granularity and pinpoint details of correctable and uncorrectable errors. There are registers to define the error severity, error logging, error mask ability and to identify source of error. PCIe advanced error reporting register structure Below are the details of some important registers required for advanced error handling. Advanced Correctable Error status register When a correctable error occurs the corresponding bit within the advanced correctable error status register is set, independent of the mask register setting. These bits are automatically set by hardware and are cleared by software when writing a "1" to the bit position. Advanced Correctable Error mask register: The correctable errors can also be masked by setting the corresponding bit in the register. Only affects the error reporting not the status bits. The masked errors are not logged in header log register and are not reported to RC. Advanced Uncorrectable Error handling registers: These errors can selectively cause the generation of an uncorrectable error message being sent to the host system. Those uncorrectable errors that are selected to be non fatal will result in a nonfatal error message being delivered and those selected as fatal errors will result in a fatal error message delivered. However, whether or not an error message is generated for a given error is specified in the advanced uncorrectable mask register. Advanced Uncorrectable Error status register: When an uncorrectable error occurs the corresponding bit within the advanced uncorrectable error status register bit is set, independent of the mask register setting. Advanced Uncorrectable Error severity register: AER mechanism

defines the error severity handling for uncorrectable errors whether which one error is the more severe. Uncorrectable Error mask register: The uncorrectable errors can also be masked by setting the corresponding bit in the register. The default condition is to generate error messages for each type of error. Errors received by the RC result in status registers being updated and the error being conditionally reported to the appropriate software handler or handlers. Root Complex Error Status register: When RC receives an error message, it sets status bits within the root error status register. This register indicates the types of errors received and also indicates when multiple errors of the same type have been received. Root Error Command Register: The root error command register enables interrupt generation for correctable or uncorrectable errors. Basic flow chart for error handling: Basic flow chart for PCIe error handling Note: A receiver without AER sends no error message for this case. For example a poisoned TLP is received by its ultimate destination, if the severity is non-fatal and the receiver deals with the poisoned data in a manner that permits continued operation, the receiver handle this case as an Advisory Non-Fatal Error. Earlier the packet at ingress port incoming port of switch is not sent to egress port out going port of switch until the tail end of packet is received and checked for CRC. In PCIe, the packet is passed from ingress port to egress port without waiting for tail end. PCIe error handling on a typical SoC: And the EP logs this error in its: And RC logs this error in its: Similarly core jump to interrupt handler corresponding to error for other errors of PCIe and take the implementation dependent actions. Requirements and recommendations for reporting multiple errors: For example suppose the DL layer detects an error, subsequent errors which occur for the same packet will not be reported by the transaction layer or suppose physical layer detects a receiver error, to avoid having this error propagate and cause subsequent errors at upper layers for example, a TLP error at the Data Link Layer , making it more difficult to determine the root cause of the error. For such case It is required and recommended that no more than one error is reported for a single received TLP, and the below precedence from highest to lowest is used:

Chapter 6 : Data logger - Wikipedia

I am currently trying to find a way to log all of the connections and disconnections of USB devices from all of the Windows machines on our network. This information needs to automatically be logged to a file on the machine, this file can then be read by nxlog and then get shipped to our centralised logging platform for processing.

Selects error-record templates with the Report field set to True. If this flag is not specified, the value from the error log configuration database is used. The ErrorID variables can be separated by a , comma , or enclosed in " " double quotation marks and separated by a , comma , or a space character. When combined with the -t flag, entries are processed from the error-template repository. Otherwise entries are processed from the error-log repository. The ErrorLabel variable values can be separated by commas or enclosed in double-quotation marks and separated by commas or blanks. When combined with the -t flag, entries are processed from the error template repository. Otherwise, entries are processed from the error log repository. This flag is used by methods in the error-notification object class. The SequenceNumber variable can be separated by a , comma , or enclosed in " " double quotation marks and separated by a , comma , or a space character. The uname -m command returns the Machine variable value. The uname -n command returns the Node variable value. The ResourceNameList variable is a list of names of resources that have detected errors. For software errors, the ResourceNameList variable lists the names of resources that have detected errors. For hardware errors, it lists names of devices or system components. It does not indicate that the component is faulty or needs replacement. Instead, it is used to determine the appropriate diagnostic modules to be used to analyze the error. The names of the ResourceNameList variable can be separated by a , comma , or enclosed in " " double quotation marks and separated by a , comma , or a space character. The -P flag applies only to duplicate errors generated by the error log device driver. The -P flag is invalid with the -D flag. For hardware errors, the ResourceTypeList variable is a device type. For software errors, it is the LPP value. The items in the ResourceTypeList variable can be each separated by a , comma , or enclosed in " " double quotation marks and separated by a , comma , or a space character. For hardware errors, the ResourceClassList variable is a device class. The -t flag can be used to view error-record templates in report form. When combined with the -t flag, entries are processed from the specified error template repository. Otherwise, entries are processed from the error log repository, using the specified error template repository. Examples To display a complete summary report, enter:

Chapter 7 : Using the Console | Tools for Web Developers | Google Developers

In Today's high speed systems PCI Express (PCIe-Peripheral Component Interconnect-express) has become the backbone. PCIe is a third generation high performance I/O bus used to interconnect peripheral devices in applications such as computing and communication platforms. It is used to provide the.

My way of troubleshooting flows this way which I will explain in detail: Isolate the issue be for user, device, server or organization wide Testexchangeconnectivity. Issue with one single user only: Have the user flip Wifi and 3G network to ensure the issue is not caused because of internet connection drop on the device or in other words, before proceeding have the user access a couple of websites on the mobile browser. Once we ensure all is well with the user, navigate to ExRCA. If this shows a pass, I would put the blame on the device and move forward. Issue with a single device only: We get this a lot. Hard part is to convince the user that its his device broke and not the server. To prove this, run ExRCA. Additionally, configure another mobile device with the user credentials and confirm that you can sync the device. Issue in a device only scenario is mostly caused because of an outdated firmware or some applications conflicting with the default EMAIL app. Have the user update the firmware on the device and if needed backup Contacts, Photos, Notes etc and reset the device to factory settings. Issue with a single server: It is important for us to understand if the issue is happening for all users or if it is isolated for users on a single mailbox server or even a mailbox database. Test-ActiveSyncConnectivity cmdlet can come handy here: If you think the issue is happening for users on one specific database, look for event â€" Database props quota error with AirSync named property in the description can be the culprit. Read more about the same here: You would know if this happened. This is a website from Microsoft where you can test external access for the following options: Your troubleshooting should start with ExRCA. Post testing, it will return the HTTP status code for the test. For every connection made by individual user or devices, there will be a respective IIS log generated on the internet facing CAS server. But how do we read it? The default location of IIS log files: Let it error out. We need to perform the next step in all Internet facing CAS servers at the same time. Scroll to the extreme bottom. In this case, it is RatishNair. Now I see the latest entry made by my mobile device: Remember the chaos created by iOS4. So no matter what if your organization contains devices running iOS 4. Official Microsoft and Apple documentation can be found here: Unable to connect using Exchange ActiveSync due to Exchange resource consumption: Exchange Mail, Contacts, or Calendars may not sync after update: This is all I could collect.

Chapter 8 : Logging devices change in device manager - Windows 7 Help Forums

With Windows Device Portal's ETW Logging tool, you can get a live view of any ETW provider on the system. Combined with the LoggingChannel APIs in WinRT, you can easily add tracing to your UWP and view that output in the comfort of your browser.

The most common IO error messages and codes are: Windows is trying to use a transfer mode that the hardware device cannot use. The hardware device that you are trying to access is damaged or defective. The hardware drivers are damaged or incompatible. There is a connection problem, such as a bad cable. Restart your computer, and then try to access the drive or disk again. Use a cleaner disc to clean the disk. If you have another computer available, try to access the data on the drive or disk with the other PC to confirm that the drive or disk is not damaged. If you do not have another computer available, try a different disk to make sure that the problem is with the computer and not with the original disk. If the problem is fixed and you no longer get the error message, you are finished. If the problem remains, continue to the next paragraph. Try these solutions in the following order: Make certain that all cables are connected correctly If the drive is an external drive, make sure that the cable that connects the computer to the drive is functioning correctly. If the cable fails, the drive will not work correctly. If you have another cable, try to use it, and also try to attach it to another USB port. Note Changing cables for an internal drive for a desktop computer is recommended only for advanced computer users, because there are many internal items that can be easily damaged. You should not try to change cables inside a laptop or portable computer. If above solutions resolved the issue, you are finished. If this did not resolve the IO issue, continue to solution 2. Start the computer in a clean boot state Try to perform a clean boot of your computer to determine whether a program or driver is having a conflict with the drive. Click the following links for more information about how to configure Windows XP or Windows Vista to start in clean boot state. If a clean boot fixes the problem, there may an incompatible program or driver on your PC. For more information, click the following links for more information about how to perform advanced clean-boot troubleshooting in Windows XP or Windows Vista. If this solution fixed the problem, you are finished. Change the transfer mode for the drive in IDE Channel Properties If the transfer mode for the drive was changed or is incorrect, Windows cannot transfer data from the drive to the computer. You can fix this problem by changing to the correct transfer mode. To change the transfer mode, follow these steps: Right-click the channel where the appropriate drive is connected, and then click Properties. Typically, this is Device 0. Then, click OK and exit all windows. Changing this transfer mode setting may cause the computer to operate incorrectly or not at all. If the problem is not resolved after you change the transfer mode for the secondary IDE channel device 0, the drive may not be located there. Use the same procedure to change the transfer mode back to DMA if available. Then, repeat steps to change the transfer mode for IDE devices in the following order until the issue is resolved: Primary IDE channel, device 1 Secondary IDE channel, device 1 After you change your settings, make sure you restart your system so that the computer recognizes the changes you have made. After you reboot, check the settings to make sure they are in effect. If they are, your device should now work properly. If this did not fix the problem, try solution 4. Check the status of the device in Device Manager You can check the status of the drive in Device Manager to ensure that the device driver is working properly. If there is a hardware problem or a software conflict preventing the device from working properly, usually Device Manager will identify the problem. Click the following links for more information about how to manage devices in Windows XP or Windows Vista. If this did not fix the problem, go to solution 5. Contact the hardware manufacturer Visit the website or get in touch with the manufacturer of the hardware device to find out whether there is a firmware or a driver update available for download. Other Solutions to Windows Errors and Slow PC Performance The best thing you can do, to stop your computer from getting more error messages or slow down your PC performance, is to repair and clean your Windows Registry. RegCure cleans, repairs and optimizes the Windows Registry in under 2 minutes.

Chapter 9 : Logging when someone connects or removes a USB device to/from a Windows machine - Sup

A simple way is to make your own log collector methods or even just an existing log collector app from the market. For my apps I made a report functionality which sends the logs to my email (or even to another place - once you get the log you can do whether you want with it).

This is assuming of course, that the device actually connects, gets past IIS, and into Exchange code. When troubleshooting EAS issues, this is often the most useful piece of information. PowerShell Method Enable the logging on the affected mailbox: The cmdlet is otherwise the same. By default, these logs will contain tags that are truncated -- the data for most tags is removed, and replaced with a tag attribute indicating how many bytes the data contains. For example, the subject of an email may look like this: To do so, open the x: No restart is required of IIS or the application pool. To enable EAS logging, open the x: Note that this setting is also per-CAS, so the traffic will only be logged if the device hits a CAS with this enabled. Other than this setting, the rest of the steps are the same as Exchange current. This slab contains a list of the EAS devices for the mailbox, and users can enable logging and retrieve it from here. Mobile devices slab in Exchange Mobile devices slab in Office In any of the versions, select the device you want logging for, and click the "Start Logging" icon highlighted in yellow. After enabling the logging, reproduce the behavior and then click "Retrieve Log" which will be the same button. Whether you use PowerShell or ECP to enable logging, the log is sent to you in an email message that has the log attached. These logs are not intended to stay enabled very long. Understanding these logs may require extensive protocol review, but some will be fairly straightforward. Sample Log Here is a snippet from a sample log showing the MeetingResponse command. Log Entry This is a sequential entry number, starting at 0. This will show if the connection is being proxied, etc. Consider this the raw request from the client. This includes some optional elements that are not required, and show the default or implied settings. AccessState The access state for this specific device. AccessStateReason The reason for the access state above. Most everything else is going to be edge-case. This is where I find many people hit a wall. You can mostly ignore the xmlns. The xmlns is the XML namespace, which at a high level specifies the specific type of MeetingResponse, and is defined in the schema , which is also in the protocol documentation. Start at the MeetingResponse command itself. Notice there is the Request and the Response. The Child elements column here lists the elements with the data we care about based on the request we see in the log. UserResponse â€” 3 possible values, indicating whether the meeting is being accepted, tentatively accepted, or declined. This request has a UserResponse of 1, meaning the meeting request was Accepted. CollectionId â€” String value specifying the folder that contains the meeting request. This value is obtained from a previous FolderSync or FolderCreate command response. The first FolderSync for the device will pull a folder list that is alphabetized, and the CollectionId is sequential. If the folders change after the FolderSync, the change to the FolderHierarchy is sent to the device, but the CollectionId just increments the number. So the newest folder gets the largest number. If the device partnership is reset, then the newest folder gets a CollectionId that is in the proper alphabetical order. RequestId â€” String value specifying the server ID of the meeting request message item. Notice the format here is colon-separated. In this case the CollectionId is 1, so the RequestId is 1: The ItemId here acts much like the CollectionId above. The number increments in the partnership, but on a new sync, the items will all be in sequential order. Unlike the FolderHierarchy, these items are not alphabetized, but in chronological order. The first item in the box oldest will be ItemId 1. The server will process the request, and send the response as shown in the ResponseBody: The Id is 1: Status â€” 4 possible values, indicating the success or failure of the MeetingResponse command. In this example the status is a 1, meaning the request was successful. CalendarId â€” String value specifying the server ID of the calendar item instead of the message object associated with the calendar item. If the meeting request is accepted, the server ID of the calendar item is returned, and is the new server ID. Every request command and response is analyzed in a similar manner.