

Common technical issues with MEE

(issues unrelated to malware removal)

Issue: User no longer remembers his or her password to log into MEE.

Cause: Most likely this user does not actually use the Management Console very often.

Resolution: In this circumstance we would either have to use a reset tool, which is actually a pretty dangerous, or make edits in the user's database to change the password. Going forward, we would recommend having multiple admin level users in the console to reduce the likelihood of one person being responsible for the console.

Issue: Client computer hangs at start or has a long login process.

Cause: This is a result of the Managed Client conflicting with something at the time the computer is going through the startup process.

Resolution: In order to resolve this issue we want to start by implementing a delayed start within the policy. This basically has the client wait for a given period of time before it goes through its startup process. The idea is to get around whatever is causing the hang to occur. Another option to resolve this would be to set the MEE services from Automatic to Automatic delayed. Without going into too many details this is similar to a delayed start, except instead of using a set time, the client now waits for Windows to tell it to start. An important note here is that adjusting the services is not available on Windows XP machines.

Issue: Clients are offline, won't accept commands, won't send logs, console runs slowly and the user may even be unable to login to the console.

Cause: The cause of this kind of behavior is an SQL database that has reached its maximum limit. This means that clients or users are unable to write to the database.

Resolution: Here we will need to educate the customer on the cause of the issue to help them better understand going forward. If the customer is using SQL Server Express, there is a hard limit of 10 GB and, honestly, this is an easy limit to reach. This user may consider upgrading to full SQL to better support his or her network. If they are already using a full version of SQL, they may wish to increase the maximum size of the MEE instance. To resolve this issue we would need to delete items from the database to make space.

This is accomplished through the use of a query that will be ran within SQL Server Management Studio. Generally, we delete from the Client Security Log table.

Issue: Customer is scanning an IP range but is unable to detect the clients.

Cause: Often this is a result of a firewall or setting that is not enabled that is preventing a client from either receiving messages from the Management Console or responding to them.

Resolution: The first thing we like to look at is the basic settings that will be required for network communication between the Management Server and the Managed Client. This includes but is not limited to: Opening ports such as the communication port 18457 and 137, enabling NetBIOS, enabling File Sharing, and enabling Remote Procedure Calls. If confirming these settings does not resolve the issue we want to look at the customer's security software and network topology. We want to find out if there is a software firewall other than Windows that might be causing issues, such a Symantec firewall or Sonicwall. Also we want to look for a physical firewall that may not even be managed by the customers themselves. In this type of situation there ends up being a good amount of investigation that is required before an actual resolution can be reached.

Issue: When performing an installation of the client software the user receives an error message indicating that the client failed to register.

Cause: This is a result of the client software not being able to contact the server for the first time.

Resolution: To function properly, every managed client needs to connect up to the Management Server at least once to register. Failing to do this will prevent the policy from taking effect on the client, which means things like scheduled scans will not start. Often we look at the basic settings, as was mentioned earlier in the document. We generally see this as a result of remote clients who do not have direct access to the Management Server. We advise all of our customers to allow remote clients to connect to the Management Server at least once through VPN or, if necessary, have them install the software locally, and then ship the laptop back to the user.

Common technical issues with MEE

(issues unrelated to malware removal)

Issue: Customer is unable to log into the console during initial setup.

Cause: The root cause of this is either a lack of documentation or a lack of information.

Resolution: The default user name and password are "Admin." This is common knowledge among the support team but whether or not the users get this knowledge is another thing. This information can be located within the Admin Guide but it requires a user to actually read it. So this issue is really one of having information easily accessible to the customer, or customers putting in some effort.

Issue: Customer is not able to install the Management Server on Windows Server 2003.

Cause: This is basic stuff here really. We only support a select number of operating systems for the Management Server and the customer is either not aware or does not care.

Resolution: If the customer would like to progress further than the initial setup of the Management Console and Server they need to switch their installation to a supported operating system. Supported operating systems are Windows Server 2008 and 2012.

Issue: Customer is finding that after deploying MEE into their network that there is a lot of network congestion that is slowing down performance.

Cause: This is often a result of all the Managed Clients being on the same policy, causing every client to try checking into the Management Server at once. When you consider 1-2kb of data every time a single client checks in, then you can see why 500 at once can cause issues.

Resolution: In this circumstance we want to create multiple groups within the client pane. Then separate the clients into these multiple groups. An easy way to separate the clients would be by department. Once the clients has been separated, we then need to create a policy for each group. Within these policies we will be editing the communication

time so that the times the clients check into the server are staggered. Choosing times like 17 minutes and 32 minutes are ideal. The idea is to reduce the likelihood of the client groups overlapping when they contact the server.

Issue: Customer does not want to install SQL Server Express or IIS.

Cause: Some customers already have their own programs or systems in place and do not want to install what they may see as an inferior product or as redundant.

Resolution: These is a little wiggle room here. IIS must be installed with the program and there isn't a way around this. However, for SQL Server Express this is not the case. There is a method for working around the prerequisite portion of the installer. When performing this process we ask that the customer install the prerequisites manually, except for SQL. Once the work around is completed, the customer can then install MEE and use their existing SQL database without having to install the express version.