Auditing of specific items in EFT

THE INFORMATION IN THIS ARTICLE APPLIES TO:

- EFT v8.0 and later

DISCUSSION

The following Advanced Properties enable or disable auditing of specific items:

- AuditBannedSocketConnections - auditing of banned socket connections. Default = true (audit); false to skip
- AuditFailedAuthforNonExistingUsernames - auditing of all invalid username authentication attempts. Set to false by default; true to audit
- AuditFailedAuthforUsernameRoot - auditing of 'root' and 'administrator' invalid username authentication attempts. Set to false by default; true to audit
- AuditFailedSocketConnectionsOther - auditing of other failed socket connections. Set to true (audit) by default; false to disable
- AuditIgnoreFailedAuthforNonExistingUsernames - auditing of usernames that are not a user in EFT; set to true to audit (introduced in EFT Arcus in v7.4.14)
- AuditIsInternal - auditing of non-CRUD (IsInternal) transactions. Set to false by default. When set to true, EFT will audit a row to protocol commands for resources that have an IsInternal flag set to 1. For example, IsInternalflag is set to 1 for HTTP protocol GET requests for reserved paths.
- AuditIsRESTAdmin - auditing of Administrative REST calls. Set to false by default; true to audit
- AuditIsRESTRAMAgent - auditing of RAM REST calls. Set to false by default; true to audit
- AuditIsRESTUSER - auditing of user-initiated REST calls. Set to false by default; true to audit
- AuditIsRESTWorkspacesInternal - auditing of Workspaces config REST calls. Set to false by default; true to audit
- AuditUnimportantCommands - auditing of unimportant (non CRUD) operations (HTTPS connections only). Set to false by default. When set to true, EFT will audit to tbl_ProtocolCommands the HTTPS commands where command is "HEAD", "SIZE", "LIST", "GET", "OPTIONS", "QUIT".
- AuditRedundantUserAndPass - auditing of username and password for S/FTP/S events. Set to true by default; true to audit
- AuditRESTWorkspaces - auditing of Workspaces REST calls. Set to False by default; true to audit

- AuditSuccessSocketConnections - auditing of successful socket connections. Set to False (don't audit) by default; true to audit

To enable these advanced properties

- Add the applicable name:value pair to the AdvancedProperties.JSON file. You can add multiple name:value pairs. For example:

{

"AuditFailedAuthforNonExistingUsernames":false

"AuditRedundantUserAndPass":false

"AuditSuccessSocketConnections":false

}

For more information about the Advanced Properties, refer to the online help for your version of EFT.