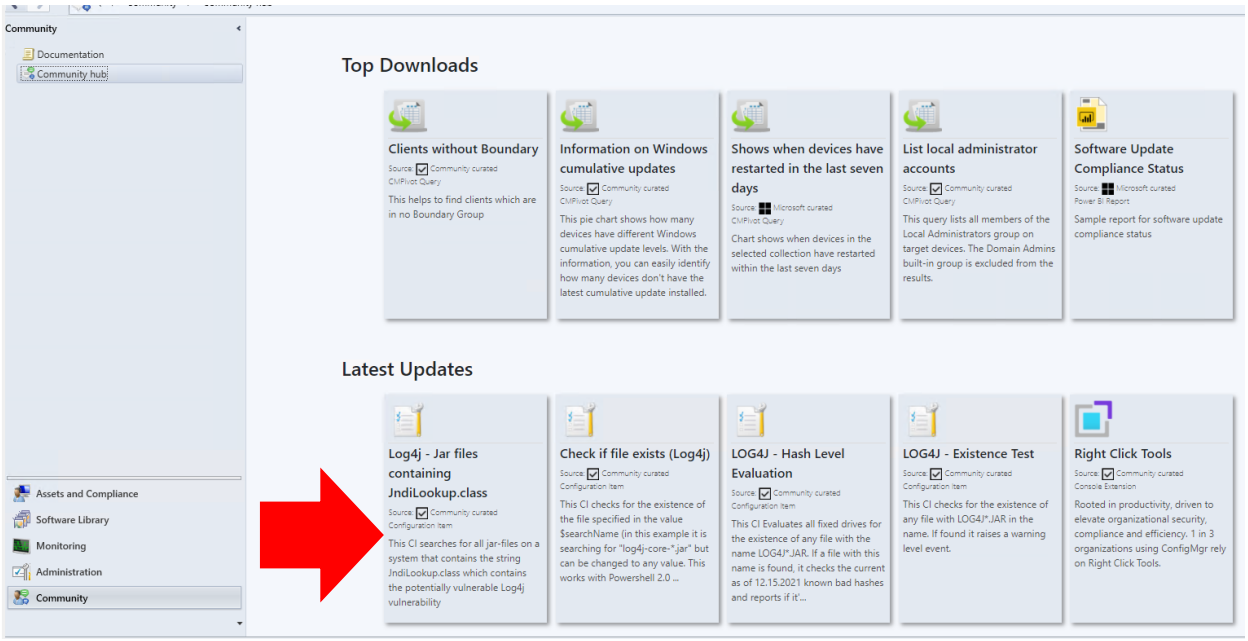
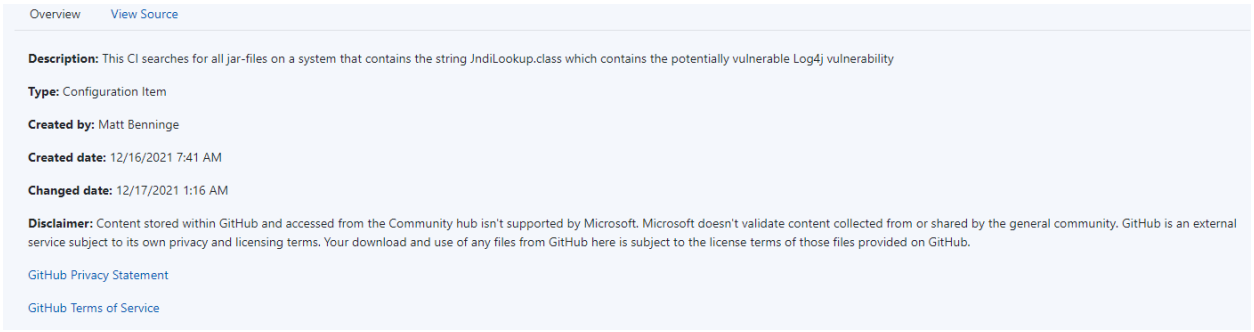
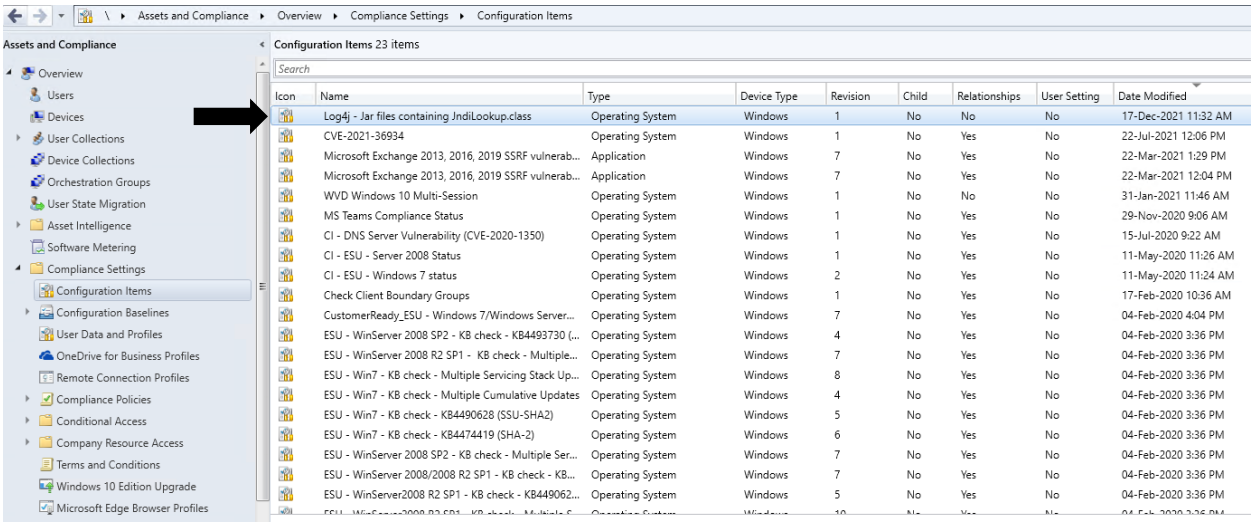
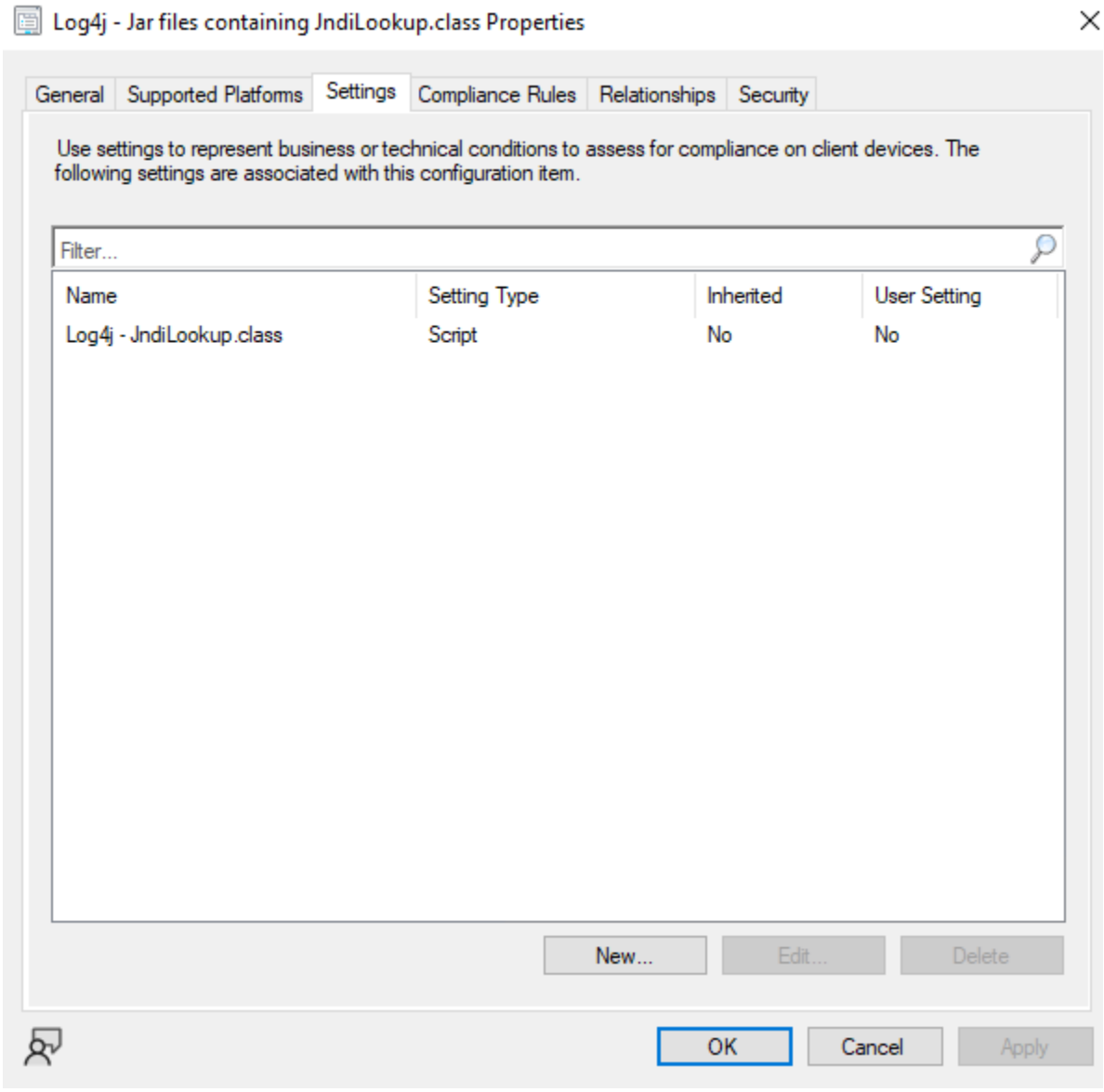
Log4j Issue -Jar files

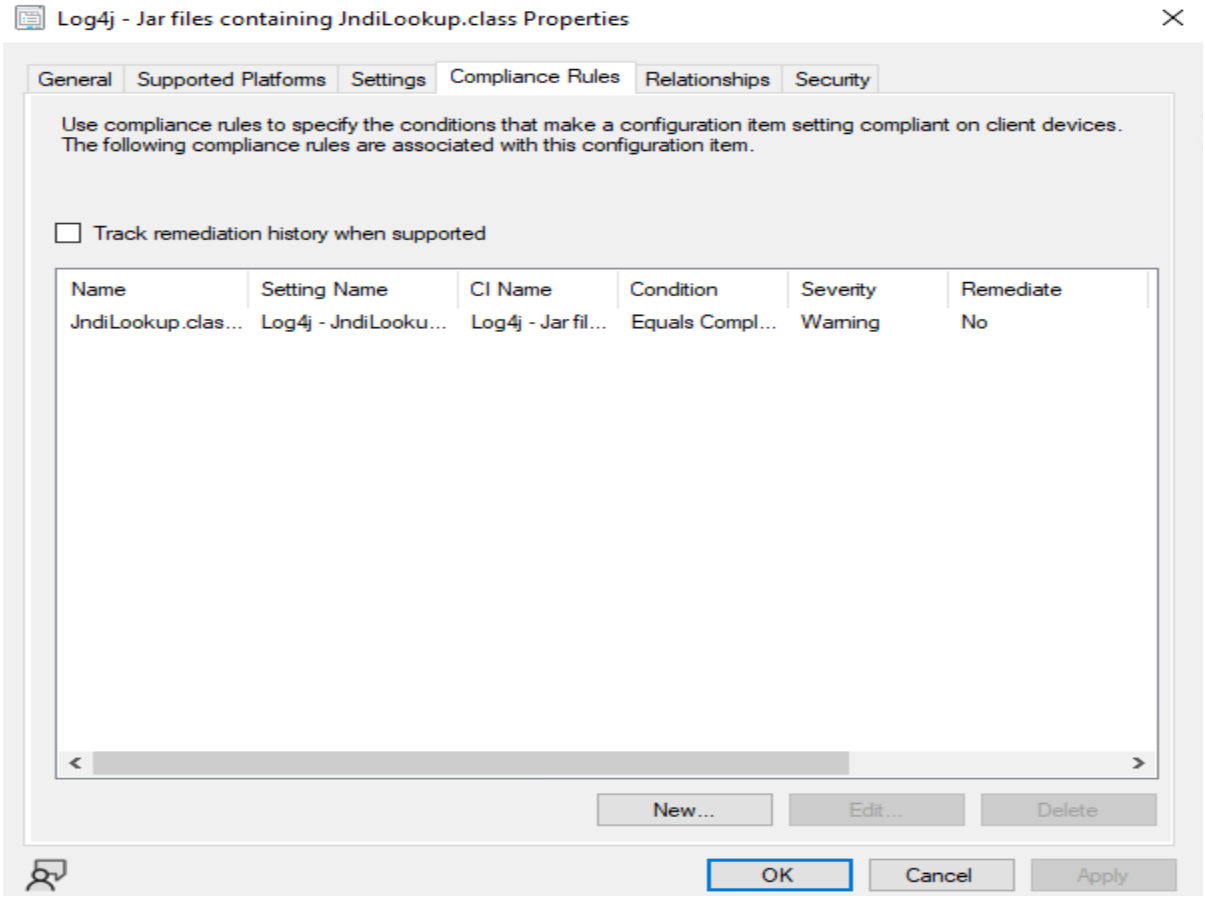
In this post, I am going to download and configure CB (Configuration Baseline) and deploy to All Systems to check and make sure there is no breach with Log4j within the network.



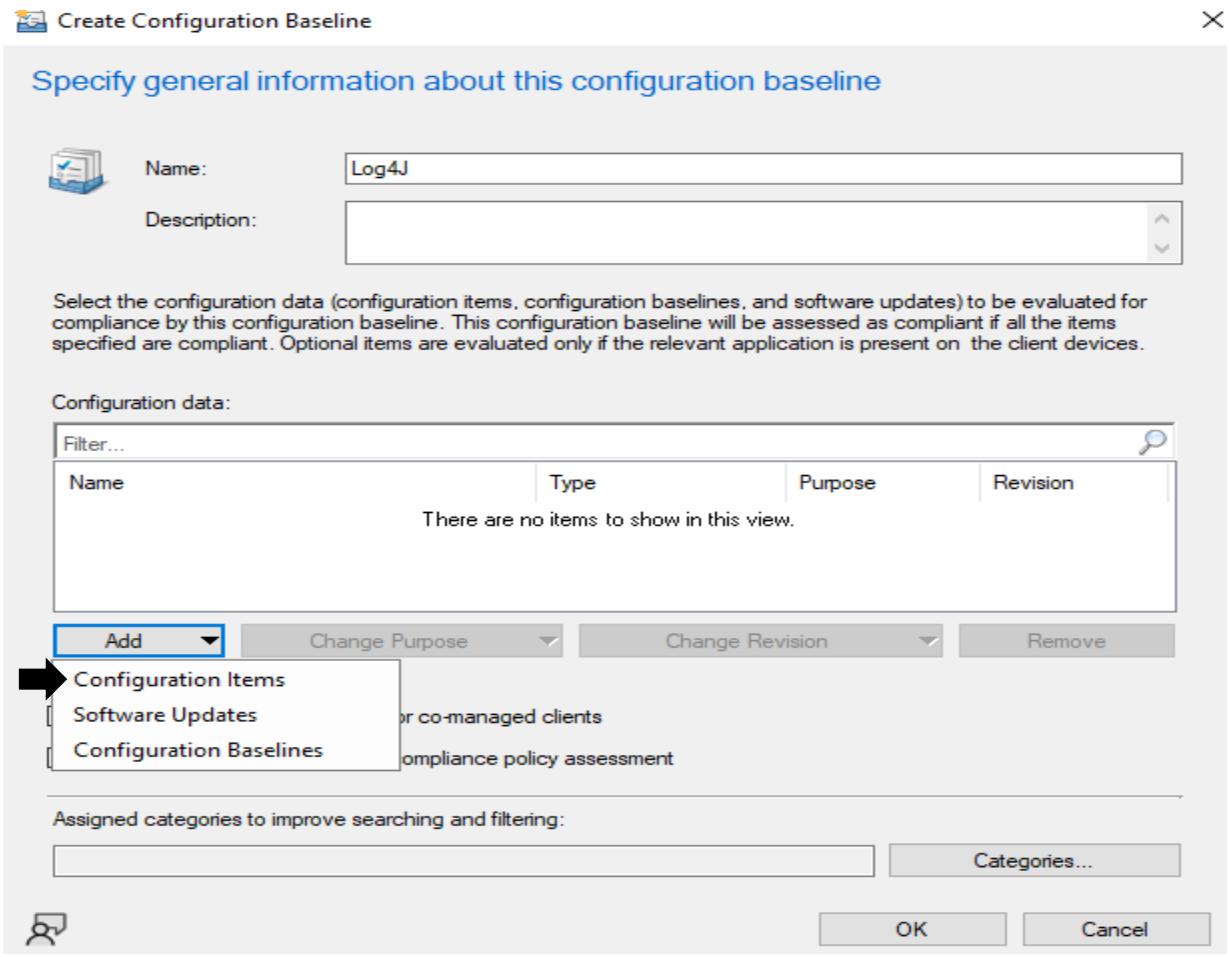


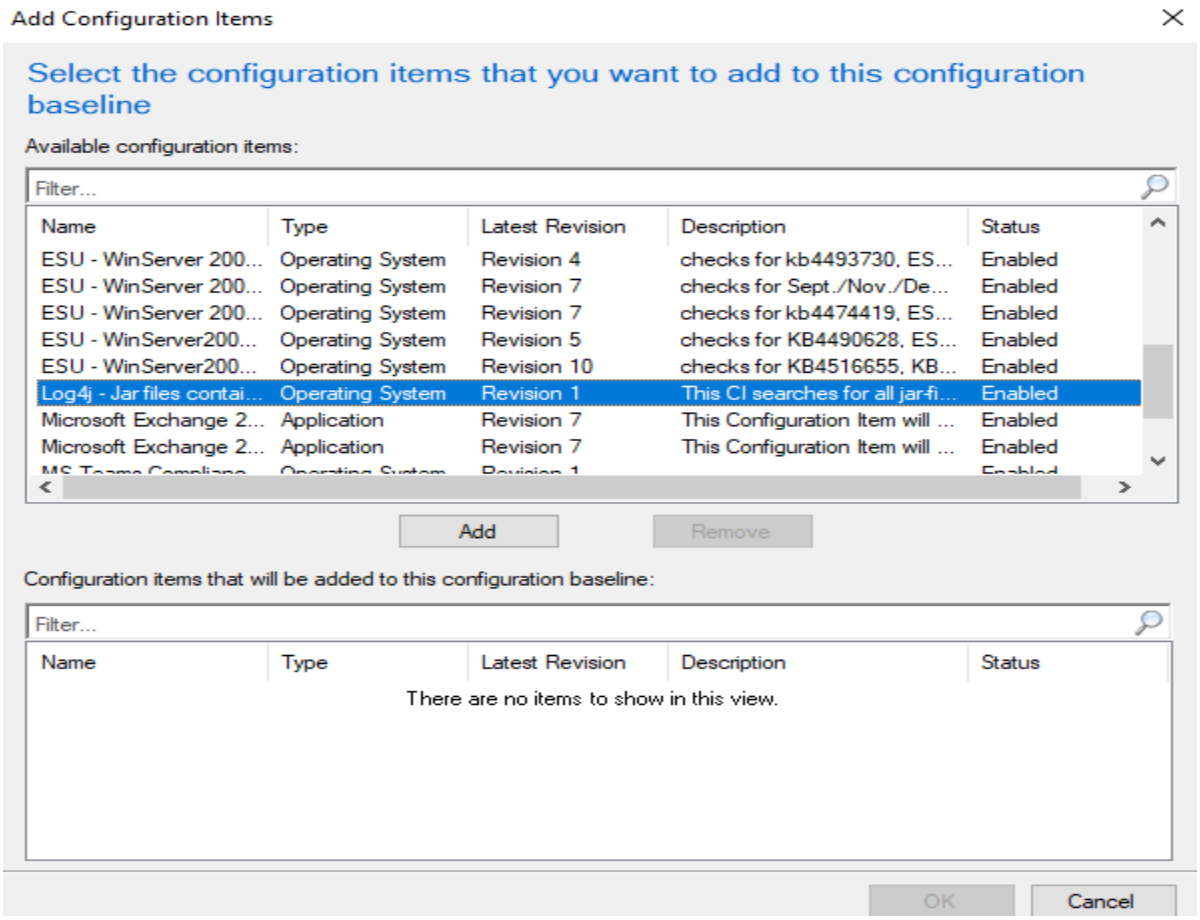

Assets and Compliance ▸ Overview ▸ Compliance Settings ▸ Configuration Items
Assets and Compliance
Overview
Users
Devices
User Collections
Device Collections
Orchestration Groups
User State Migration
Asset Intelligence
Software Metering
Compliance Settings
Configuration Items
Configuration Baselines
User Data and Profiles
OneDrive for Business Profiles
Remote Connection Profiles
Compliance Policies
Conditional Access
Company Resource Access
Terms and Conditions
Windows 10 Edition Upgrade
Microsoft Edge Browser Profiles
Configuration Items 23 items
Search
Icon | Name | Type | Device Type | Revision | Child | Relationships | User Setting | Date Modified
Log4j - Jar files containing JndiLookup.class | Operating System | Windows | 1 | No | No | No | 17-Dec-2021 11:32 AM
CVE-2021-36934 | Operating System | Windows | 1 | No | Yes | No | 22-Jul-2021 12:06 PM
Microsoft Exchange 2013, 2016, 2019 SSRF vulnerab... | Application | Windows | 7 | No | Yes | No | 22-Mar-2021 1:29 PM
Microsoft Exchange 2013, 2016, 2019 SSRF vulnerab... | Application | Windows | 7 | No | Yes | No | 22-Mar-2021 12:04 PM
WVD Windows 10 Multi-Session | Operating System | Windows | 1 | No | No | No | 31-Jan-2021 11:46 AM
MS Teams Compliance Status | Operating System | Windows | 1 | No | Yes | No | 29-Nov-2020 9:06 AM
CI - DNS Server Vulnerability (CVE-2020-1350) | Operating System | Windows | 1 | No | Yes | No | 15-Jul-2020 9:22 AM
CI - ESU - Server 2008 Status | Operating System | Windows | 1 | No | Yes | No | 11-May-2020 11:26 AM
CI - ESU - Windows 7 status | Operating System | Windows | 2 | No | Yes | No | 11-May-2020 11:24 AM
Check Client Boundary Groups | Operating System | Windows | 1 | No | Yes | No | 17-Feb-2020 10:36 AM
CustomerReady_ESU - Windows 7/Windows Server... | Operating System | Windows | 7 | No | Yes | No | 04-Feb-2020 4:04 PM
ESU - WinServer 2008 SP2 - KB check - KB4493730 (... | Operating System | Windows | 4 | No | Yes | No | 04-Feb-2020 3:36 PM
ESU - WinServer 2008 R2 SP1 - KB check - Multiple... | Operating System | Windows | 7 | No | Yes | No | 04-Feb-2020 3:36 PM
ESU - Win7 - KB check - Multiple Servicing Stack Up... | Operating System | Windows | 8 | No | Yes | No | 04-Feb-2020 3:36 PM
ESU - Win7 - KB check - Multiple Cumulative Updates | Operating System | Windows | 4 | No | Yes | No | 04-Feb-2020 3:36 PM
ESU - Win7 - KB check - KB4490628 (SSU-SHA2) | Operating System | Windows | 5 | No | Yes | No | 04-Feb-2020 3:36 PM
ESU - Win7 - KB check - KB4474419 (SHA-2) | Operating System | Windows | 6 | No | Yes | No | 04-Feb-2020 3:36 PM
ESU - WinServer 2008 SP2 - KB check - Multiple Ser... | Operating System | Windows | 7 | No | Yes | No | 04-Feb-2020 3:36 PM
ESU - WinServer 2008/2008 R2 SP1 - KB check - KB... | Operating System | Windows | 7 | No | Yes | No | 04-Feb-2020 3:36 PM
ESU - WinServer2008 R2 SP1 - KB check - KB449062... | Operating System | Windows | 5 | No | Yes | No | 04-Feb-2020 3:36 PM

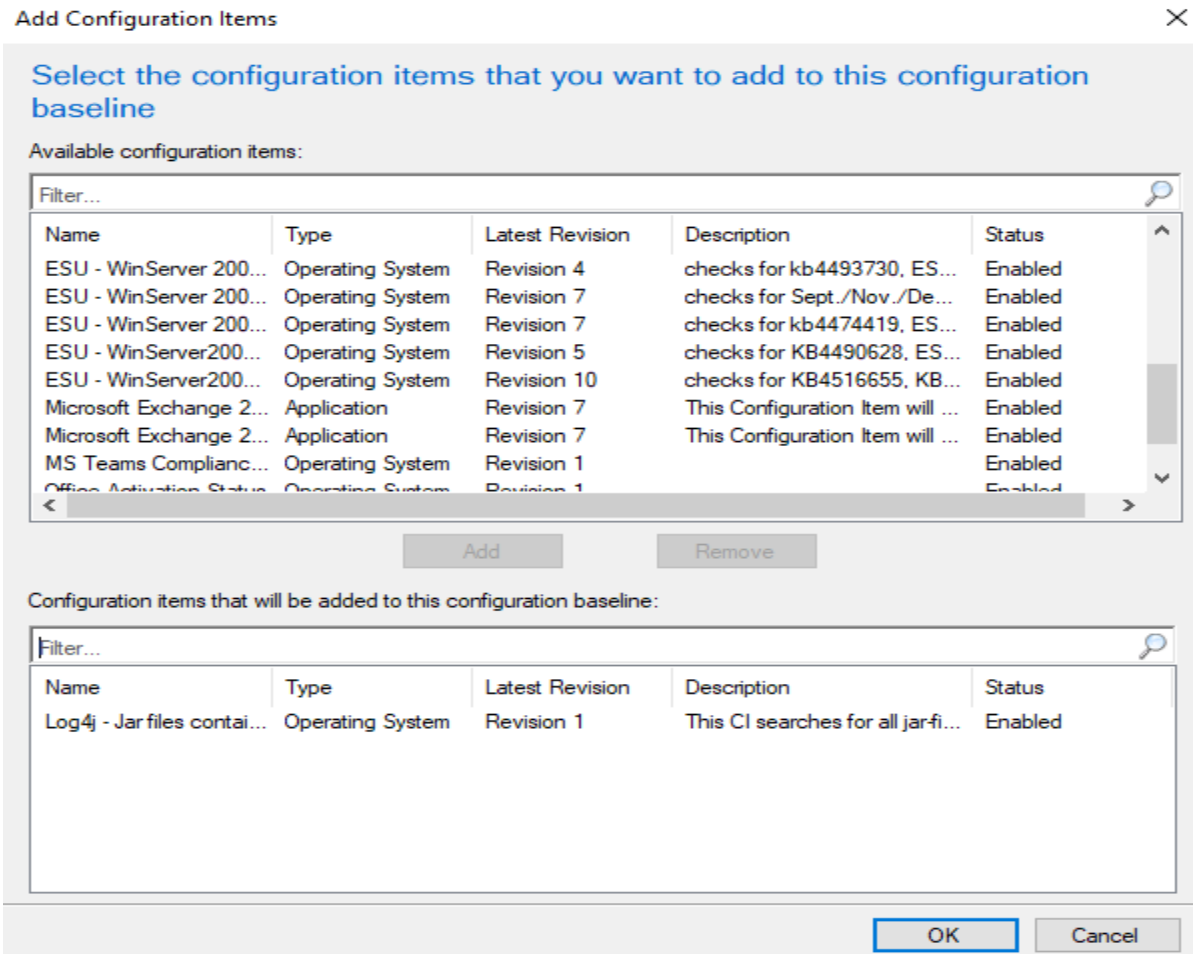

Log4j - Jar files containing JndiLookup.class Properties
General
Supported Platforms
Settings
Compliance Rules
Relationships
Security
Use settings to represent business or technical conditions to assess for compliance on client devices. The following settings are associated with this configuration item.
Filter...
Name | Setting Type | Inherited | User Setting
Log4j - JndiLookup.class | Script | No | No
New...
Edit...
Delete
OK
Cancel
Apply

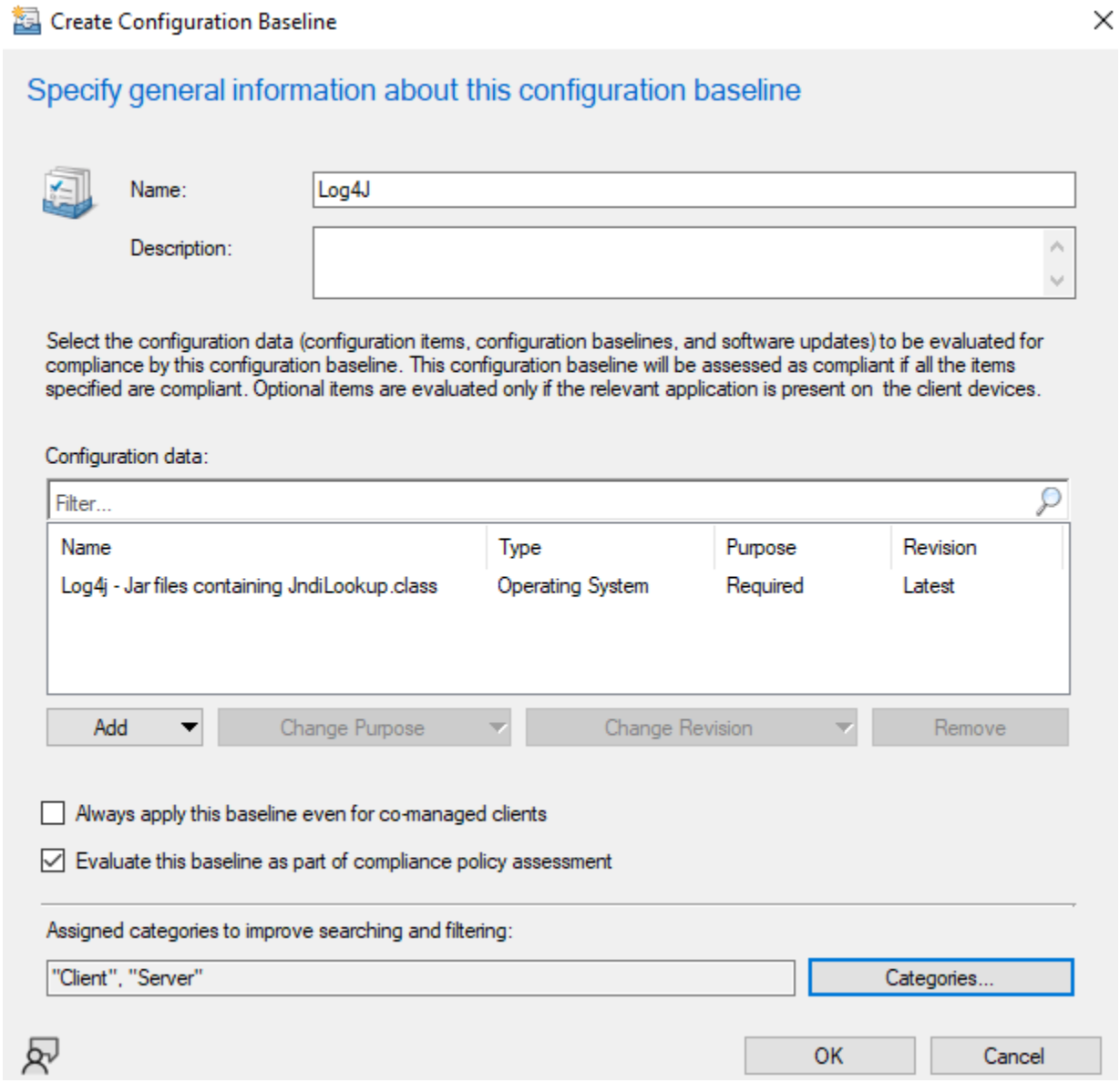


Will create Configuration Baseline

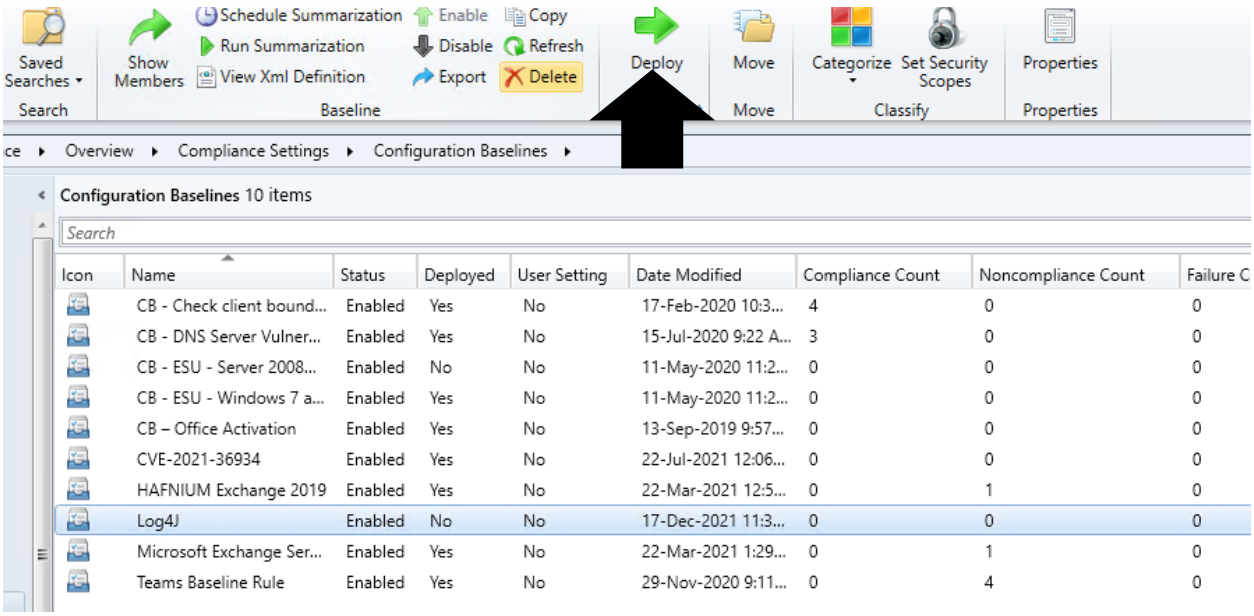


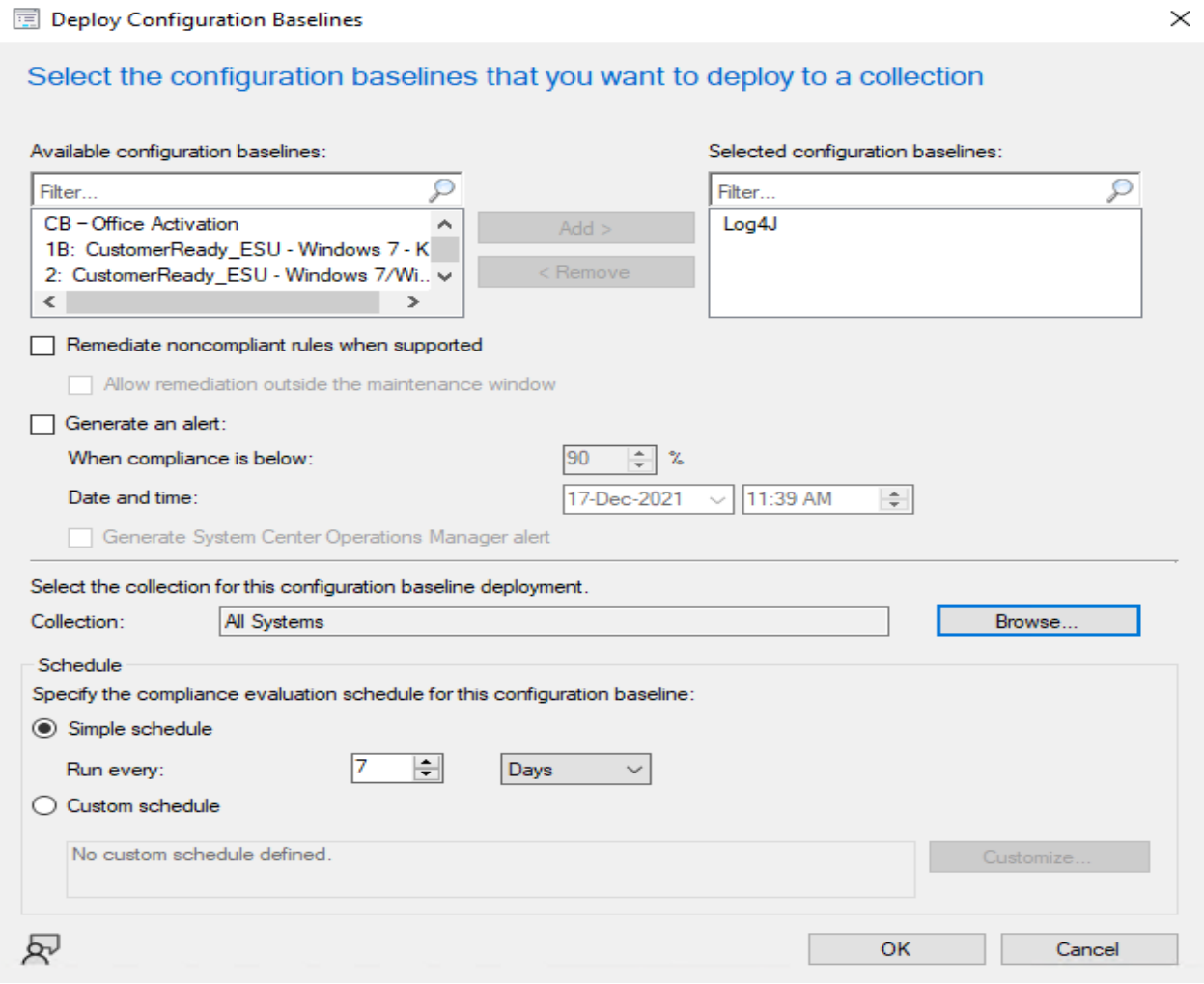

Add Configuration Items
Select the configuration items that you want to add to this configuration baseline
Available configuration items:
Filter...
Name Type Latest Revision Description Status
ESU - WinServer 200... Operating System Revision 4 checks for kb4493730, ES... Enabled
ESU - WinServer 200... Operating System Revision 7 checks for Sept./Nov./De... Enabled
ESU - WinServer 200... Operating System Revision 7 checks for kb4474419, ES... Enabled
ESU - WinServer200... Operating System Revision 5 checks for KB4490628, ES... Enabled
ESU - WinServer200... Operating System Revision 10 checks for KB4516655, KB... Enabled
Log4j - Jar files contai... Operating System Revision 1 This CI searches for all jar-fi... Enabled
Microsoft Exchange 2... Application Revision 7 This Configuration Item will ... Enabled
Microsoft Exchange 2... Application Revision 7 This Configuration Item will ... Enabled
Add
Remove
Configuration items that will be added to this configuration baseline:
Filter...
Name Type Latest Revision Description Status
There are no items to show in this view.
OK
Cancel


Add Configuration Items
Select the configuration items that you want to add to this configuration baseline
Available configuration items:
Filter...
Name Type Latest Revision Description Status
ESU - WinServer 200... Operating System Revision 4 checks for kb4493730, ES... Enabled
ESU - WinServer 200... Operating System Revision 7 checks for Sept./Nov./De... Enabled
ESU - WinServer 200... Operating System Revision 7 checks for kb4474419, ES... Enabled
ESU - WinServer200... Operating System Revision 5 checks for KB4490628, ES... Enabled
ESU - WinServer200... Operating System Revision 10 checks for KB4516655, KB... Enabled
Microsoft Exchange 2... Application Revision 7 This Configuration Item will ... Enabled
Microsoft Exchange 2... Application Revision 7 This Configuration Item will ... Enabled
MS Teams Complianc... Operating System Revision 1 Enabled
Add
Remove
Configuration items that will be added to this configuration baseline:
Filter...
Name Type Latest Revision Description Status
Log4j - Jar files contai... Operating System Revision 1 This CI searches for all jar-fi... Enabled
OK
Cancel

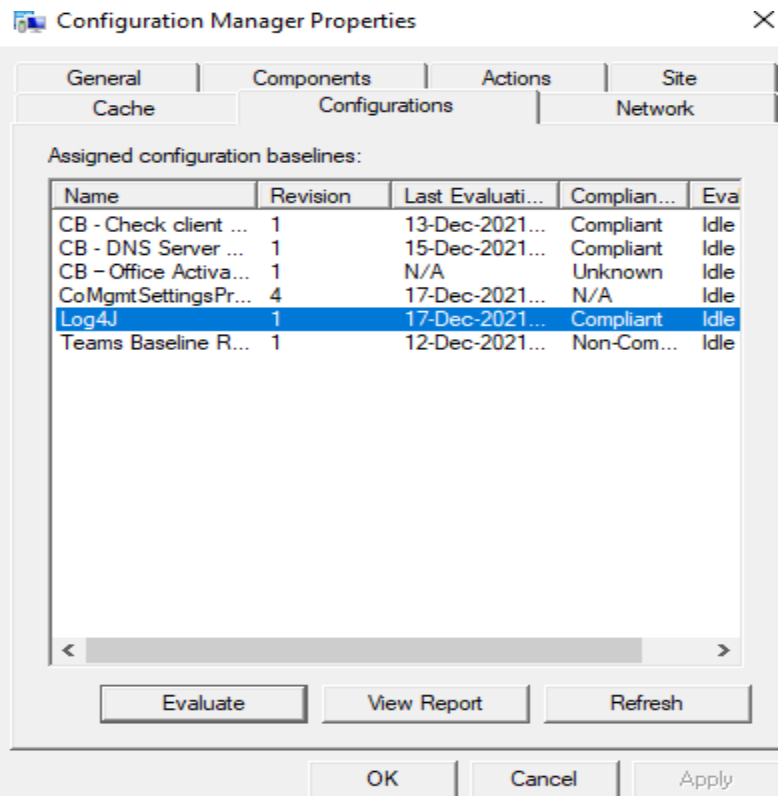


Now deploy Configuration Baseline to All Systems

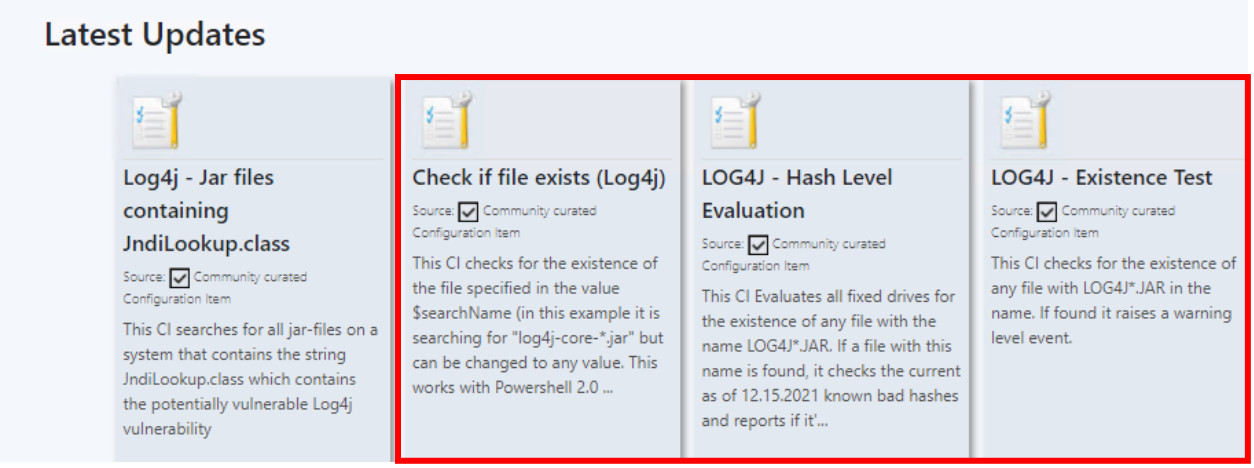


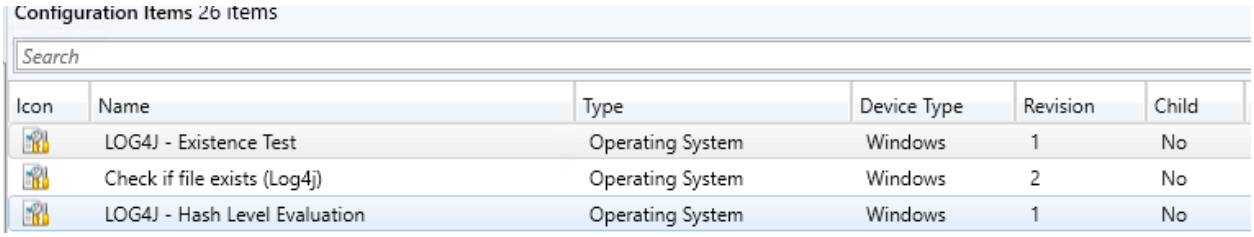


You can monitor from Control Panel – Configurations – Make sure to run Machine and User policy cycle, so it will show up in Configuration as Compliant.

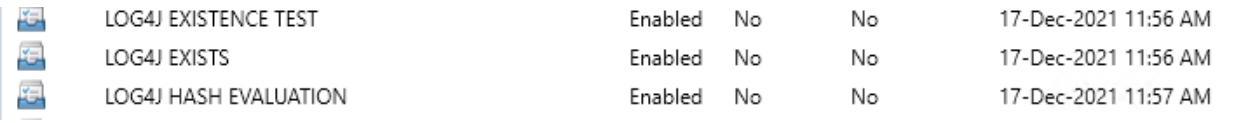


Repeat above steps for these as well.

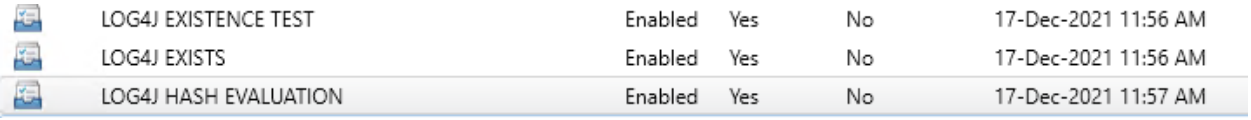




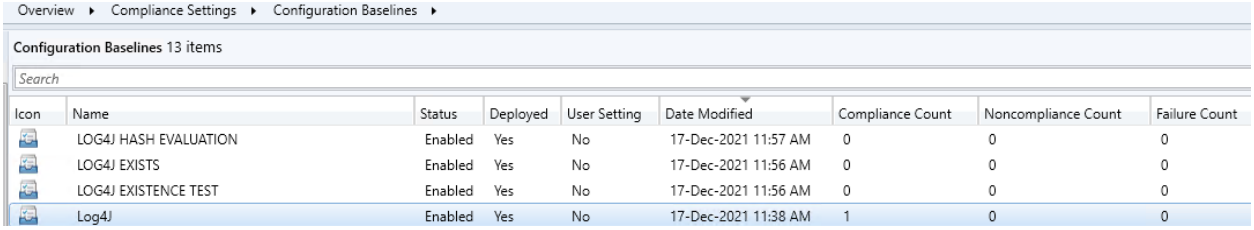
Created Configuration Baseline for above.

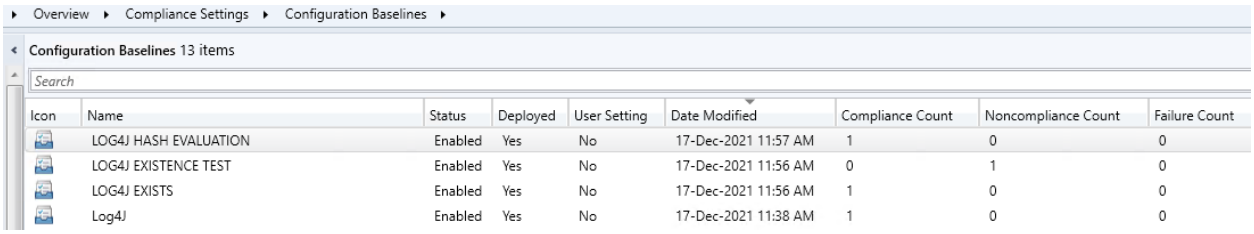


Deployed Configuration Baseline to All Systems



Here it will display whether client/server are Compliant or Non Compliant.





This concludes Log4j CI and CB.

Thanks

Ram
17th Dec 2021