ATP Configuration Process

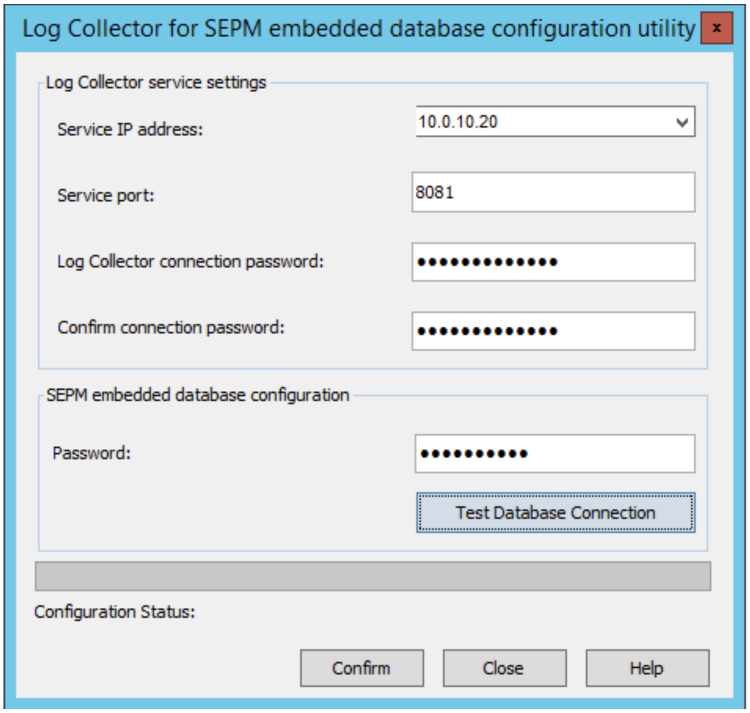
To configure ATP users should browse to the following URL: https://10.0.90.50 from the SEPM system.

ATP UI Login:
User: Admin
Pass: Symc4now!

ATP needs to be configured to connect to the SEPM. ATP has only been bootstrapped at this point.
Note* ATP may not have been started when the lab was deployed. If you are not able to see the login screen – make sure the ATP system is started via the https://labs.symantec.com interface.

RDP to the SEPM system and Configure ATP:

1. Log into ATP (https://10.0.90.50)
2. Goto Global Settings
3. Browse to the Synapse Section:
4. Select “Download Synapse Log Collector for SEPM Embedded DB”
5. Run install as **Admin** while logged into the SEPM system
    a. Launch “cmd-as-admin” from the desktop
    b. Type: cd “c:\users\testuser.CLOUD\downloads”
    c. Type: SEPMLogCollector.msi
    d. Provide the log collector configuration information:
    e. Service IP Address: 10.0.10.20
    f. Service Port: 8081
    g. Log Collector Connection Password: <SET PASSWORD>
    h. SEPM Embedded Password: P@ssw0rd9!



Log Collector for SEPM embedded database configuration utility

Log Collector service settings

Service IP address: 10.0.10.20

Service port: 8081

Log Collector connection password: ••••••••••••••

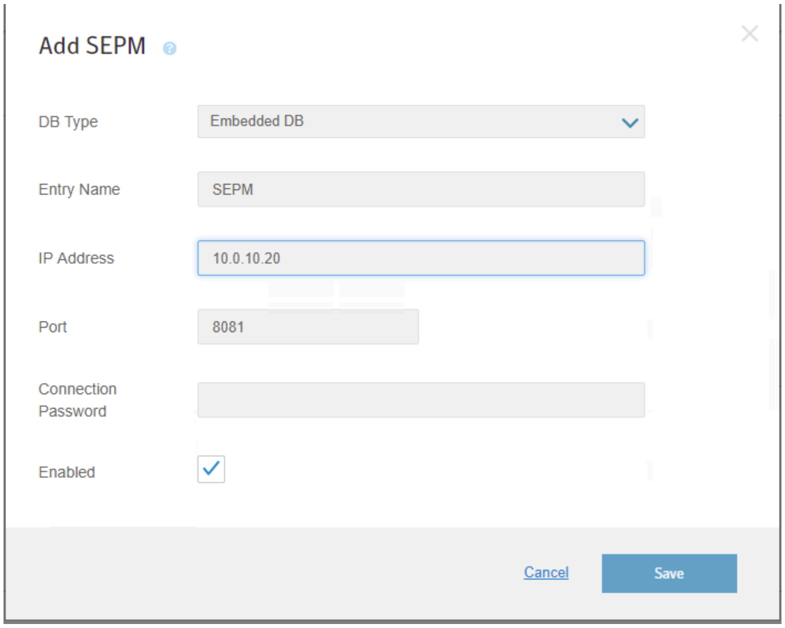
Confirm connection password: ••••••••••••••

SEPM embedded database configuration

Password: •••••••••••

Configuration Status:

6. Select “Enable Symantec Endpoint Protection Correlation”
7. Select Add SEPM and configure with the following settings:
    a. DB Type: Embedded DB
    b. Entry Name: SEPM
    c. IP Address: 10.0.10.20
    d. Port 8081
    e. Password: <USE ABOVE PASSWORD>



Add SEPM

DB Type: Embedded DB

Entry Name: SEPM

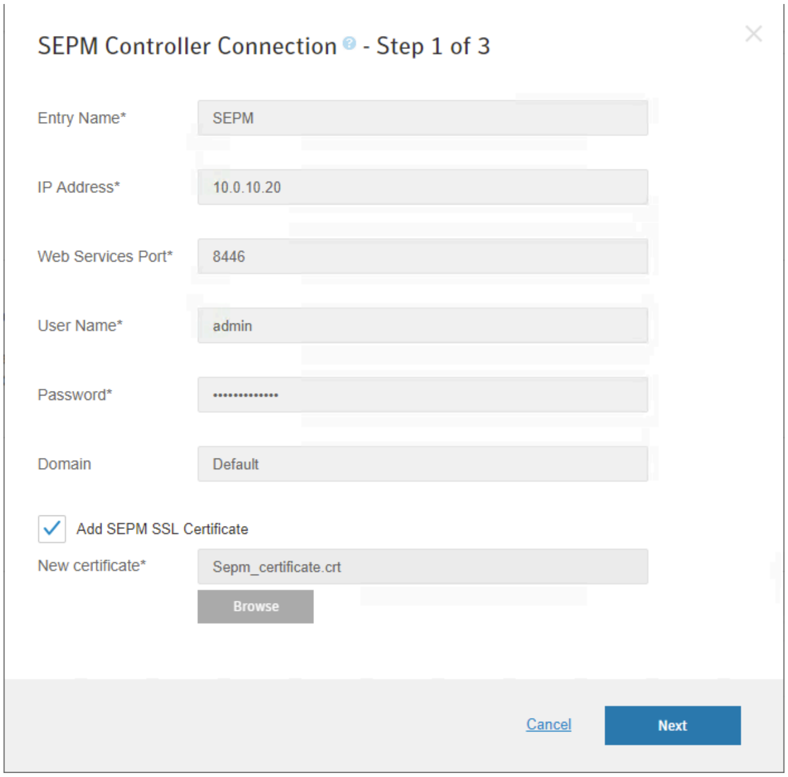
IP Address: 10.0.10.20

Port: 8081

Connection Password:

Enabled: ☑

8. Download the SEPM SSL Cert from https://127.0.0.1:8443
9. In the EDR section:
    a. Select Configure SEPM Controller
    b. Entry Name: SEPM
    c. IP Address: 10.0.10.20
    d. Web Service Port: 8446
    e. User Name: Admin
    f. Password: $ymP@ssw0rd9!
    g. Select “Add SEPM SSL Certificate” and browse the file downloaded from above.



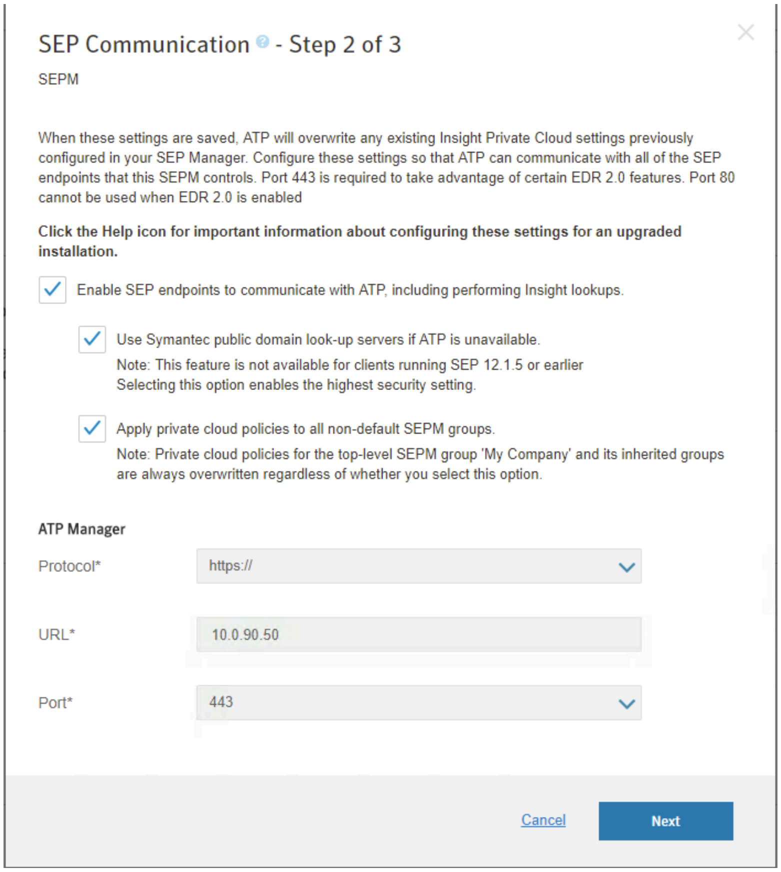
SEPM Controller Connection - Step 1 of 3

Entry Name*	SEPM
IP Address*	10.0.10.20
Web Services Port*	8446
User Name*	admin
Password*	•••••••••••••
Domain	Default

☑ Add SEPM SSL Certificate

New certificate*	Sepm_certificate.crt

10. Enable “Apply private cloud polices to all non-default SEPM groups”



SEP Communication - Step 2 of 3

SEPM

When these settings are saved, ATP will overwrite any existing Insight Private Cloud settings previously configured in your SEP Manager. Configure these settings so that ATP can communicate with all of the SEP endpoints that this SEPM controls. Port 443 is required to take advantage of certain EDR 2.0 features. Port 80 cannot be used when EDR 2.0 is enabled

Click the Help icon for important information about configuring these settings for an upgraded installation.

☑ Enable SEP endpoints to communicate with ATP, including performing Insight lookups.

☑ Use Symantec public domain look-up servers if ATP is unavailable.
Note: This feature is not available for clients running SEP 12.1.5 or earlier
Selecting this option enables the highest security setting.

☑ Apply private cloud policies to all non-default SEPM groups.
Note: Private cloud policies for the top-level SEPM group 'My Company' and its inherited groups are always overwritten regardless of whether you select this option.

ATP Manager

Protocol* https://

URL* 10.0.90.50

Port* 443

11. Configure the rest of the EDR settings as needed.
12. Log into Victim1 and test by opening the Space-Science shortcut on the desktop and browse the page.