IEM Policy Configuration

June 13, 2016

Chapter Overview

This chapter explains how to create and apply a policy for REM in the IEM.

Topics in this chapter include:

- "Create and Apply a Policy for REM in the IEM"

Create and Apply a Policy for REM in the IEM

The Interactive Experience Manager (IEM) manages the Interactive Experience Clients (IECs) at the customer pods using policies that are applied to the IEC devices.

Note Each IEC 4600 Series has its own local set of configuration settings, known as a 'Device Profile'. The device profile is useful in some applications where an IEC 4600 Series device is not managed by an IEM. In the Remote Expert Smart Solution, the IEC 4600 Series devices are always controlled by the IEM. Therefore the device policy assigned to the IEC 4600 Series device by the IEM takes precedence over any local profile information.

Refer to the *Cisco Interactive Experience Manager (IEM) Installation Guide* and the *Cisco Interactive Experience Manager (IEM) Administration Guide* to perform the following tasks:

Step 1 Install the IEM software on the VM.

Step 2 Configure the IEM server settings.

Note For the IECs to work properly, the "Device gateway", "AMF gateway", and "XML gateway" must be enabled in the IEM.

Step 3 Add an account on the IEM that will be used to manage the IECs for REM.

Step 4 Add the IEC devices to the IEM so that they can be managed by it.

Step 5 Create a new policy in the IEM for the IECs and configure the following properties in that policy to set the startup URL as well as enable or disable network failure and timeout, watchdog features, and the IEC web cache features:

- browser > startup URL = **https://<REM_IP>:8443/reic**
- browser > network > failover > enabled = **true**
- browser > network > timeout > enabled = **false**
- browser > watchdog > enabled = **false**
- browser > cache > web > enabled = **true**
- clock > NTP = NTP server IP addresses
- clock > timezone = the server's time zone

Note If the customer pods in this Remote Expert Smart Solution deployment span multiple time zones, then multiple device policies need to be created (e.g. Francisco-EST and Francisco-PST) and assigned to the appropriate IEC 4600 Series device located in those time zones.

Step 6 Apply the policy to the IECs.

Step 7 Clear IEC media and web cache in IEM.

Step 8 Reboot the IECs from REAC so that the settings will be enforced on the IECs.