# Field Reference for Service Pages

This section provides descriptions of the fields found under the **Services** tab in Cisco Prime Infrastructure.



# Guest User Field Descriptions

The following topics describe the fields on the **Services > Guest User > Add Guest User > New Controller Template** page.



## Guest User > Add Guest User > New Controller Template > General Tab

The following table describes the fields on **Services > Guest User > Add Guest User > New Controller Template > General**.

***Table 1: Guest User > Add Guest User > New Controller Template > General Tab Field Descriptions***

| Field | Description |
|---|---|
| User Name | Enter a guest username. The maximum size is 24 characters. |
| Generate Password | Select the check box to generate a username and password on every schedule of guest user account creation. If this is enabled, a different password is supplied for each day (up to the number of days chosen). If this is disabled (unselected), one password is supplied for a span of days. The generation of a new password on every schedule is optional. |

| Field | Description |
|---|---|
| Password | Enter a password. Password requirements include the following:<br>• The password must have a minimum of eight characters.<br>• The password must include at least three of the following elements: lowercase letters, uppercase letters, numbers, or special characters. |
| Confirm Password | Reenter the password that you entered in the Password field. |
| Description | Enter a description of the guest user template. |
| Disclaimer | The default disclaimer text. |
| Make this Disclaimer Default | Select the check box to set the disclaimer text as the default for this guest user template. |

# Guest User > Add Guest User > New Controller Template > Advanced Tab

The following table describes the fields on **Operate** > **Operational Tools** > **Wireless** > **Guest User** > **Add Guest User** > **New Controller Template** > **Advanced**.

***Table 2: Guest User > Add Guest User > New Controller Template > Advanced Tab Field Descriptions***

| Field | Description |
|---|---|
| Import From File | Select the check box to import bulk guest user templates. |
| Profile | Select the profile to which the guest users would connect. |
| User Role | Choose a user role for the guest user from the drop-down list. User roles are predefined by the administrator and are associated with the access of the guest (such as contractor, customer, partner, vendor, visitor, and so on).<br>User Role is used to manage the amount of bandwidth allocated to specific users within the network. |
| Life Time | Define how long the guest user account remains active by choosing one of the following options:<br>• Limited—Choose the period of time that the guest user account is active using the hours and minutes drop-down lists. The default value for Limited is one day (8 hours).<br>• Unlimited—There is no expiration date for the guest account.<br>**Note** If you choose Unlimited when configuring the guest account for Cisco Catalyst 3850 Switches (Cisco IOS XE 3.2.1) and Cisco 5760 Wireless LAN Controllers, the maximum time period that the guest account will be active is one year. |
| Apply to | From the drop-down list, choose one of the following:<br>• **Indoor Area**—Campus, Building, and Floor.<br>• **Outdoor Area**—Campus, Outdoor Area.<br>• **Controller List**—List of controller(s) on which the selected profile is created.<br>• **Config Groups**—Config group names configured on Prime Infrastructure. |

# Field Reference: Filter Options in Performance Routing Page

The following table describes about the different filter options available in the PfR Monitoring Page.

***Table 3: Filter Options***

| Filter Options | Description |
|---|---|
| **Time Filter** | • The default filter time is 72 hours. You can choose any of the preset filter time.<br>• The **Custom** option allows you to select the **From** and **To** dates and time. You cannot select a time which is less than one hour in the Custom option. |
| VRF Filter | • Allows you to select the VRF discovered by the border routers.<br>• Only the VRFs participating in the PfR controlled network are listed under this filter. |
| **Location Group filter** | • Allows you to select the **From Site** and **To Site**.<br>• You can select either a parent site or a child site. If you select a parent site, the PfR events table will display the details of the parent and all its children. |
| **Events Filter** | You can choose one or more of the following events:<br>• TCA—Generated by the primary controller whenever there is a violation of the metrics such as Unreachability, Delay, Jitter and Packet loss, based on the DSCP. You can also choose one of the TCA metrics.<br>The selection of the metrics affects only Events table, but not the Metrics Panel.<br>• RC—Generated by the primary controller whenever there is a route change to rectify a TCA.<br>• IME— Generated by the primary controller whenever an RC fails and the traffic violation could not be corrected. |
| DSCP Filter | You can choose from one of the DSCPs that are identified by the PfR. |
| **Service Provider Filter** | • Displays the list of service providers based on the border router NetFlow data and allows to select one or more service provider. |

# Field Reference for Mobility Service Engine (MSE) Pages

The following topics describe the fields on the MSE pages:

- Field Reference: MSE Location Parameters
- Filed Reference: MSE Notification Parameters
- Field Reference for MSE Alarm Detail Page

- Field Reference for MSE Clients Page
- Field Reference: Context Aware Partner and Tag Engine Status for MSE

# Field Reference: MSE Location Parameters

The following table describes the fields in **Services > Mobility Services > Mobility Services Engines >Context Aware Service > Location Parameters**.

***Table 4: Location Parameters***

| Field | Description |
|---|---|
| **General** | |
| Enable Calculation Time | Select the check box to enable the calculation of the time required to compute location.<br>**Caution** Enable only under Cisco TAC personnel guidance because enabling this field slows down overall location calculations. |
| Enable OW Location | Select the check box to enable Outer Wall (OW) calculation as part of location calculation.<br>**Note** The OW Location parameter is ignored by the location server. |
| Relative discard RSSI time | Enter the number of minutes since the most recent RSSI sample after which RSSI measurement should be considered stale and discarded. Default value is 3. Allowed values range from 0 to 99999. A value of less than 3 is not recommended. |
| Absolute discard RSSI time | Enter the number of minutes after which RSSI measurement should be considered stale and discarded, regardless of the most recent sample. Default value is 60. Allowed values range from 0 to 99999. A value of less than 60 is not recommended. |
| RSSI Cutoff | Enter the RSSI cutoff value, in decibels (dBs) with respect to one (1) mW (dBm), preceding which the mobility service always use the access point measurement. Default value is -75.<br>**Note** When 3 or more measurements are available preceding the RSSI cutoff value, the mobility service discards any weaker values and use the 3 (or more) strongest measurements for calculation; however, when only weak measurements following the RSSI cutoff value are available, those values are used for calculation.<br>**Caution** Modify only under Cisco TAC personnel guidance. Modifying this value can reduce the accuracy of location calculation. |
| Enable Location Filtering | If enabled, the location filter is applied only for client location calculation.<br>Enabling location filter allows previous location estimates to be used in estimating current location. This reduces location jitter for stationary clients and improve tracking for mobile clients. |
| Chokepoint Usage | Select the check box to enable the usage of chokepoint proximity to determine location. Applies to Cisco-compatible Tags capable of reporting chokepoint proximity. |
| Use Chokepoints for Interfloor conflicts | Allows the use of chokepoints to determine the correct floor during Interfloor conflicts.<br>Choose **Never**, **Always**, or **Floor Ambiguity**. |

| Field | Description |
|---|---|
| Chokepoint Out of Range Timeout | After a Cisco-compatible Tag leaves a chokepoint proximity range, this is the timeout (in seconds) after which RSSI information is used again to determine location. |
| Absent Data Cleanup Interval | Enter the interval period (in minutes) for removing inactive elements from the database. |
| Use Default Heatmaps for Non Cisco Antennas | Select this check box to enable the usage of default heatmaps for non-Cisco antennas during the Location Calculation. This option is disabled by default. |
| **Movement Detection** | |
| Individual RSSI change threshold | This field specifies the Individual RSSI movement recalculation trigger threshold.<br>Enter a threshold value between 0-127 dBm.<br>Do not modify without Cisco TAC guidance. |
| Aggregated RSSI change threshold | This field specifies the Aggregated RSSI movement recalculation trigger threshold.<br>Enter a threshold value between 0-127 dBm.<br>It should not be modified without Cisco TAC guidance. |
| Many new RSSI change percentage threshold | This field specifies Many new RSSI movement recalculation trigger threshold in percentage.<br>It should not be modified without Cisco TAC guidance. |
| Many missing RSSI percentage threshold | This field specifies Many missing RSSI movement recalculation trigger threshold in percentage.<br>It should not be modified without Cisco TAC guidance. |

# Filed Reference: MSE Notification Parameters

The following table describes the fields in **Services > Mobility Services > Mobility Services Engines> Notification Parameters**.

***Table 5: User-Configured Conditional and Northbound Notifications Parameters***

| Field | Configuration Options |
|---|---|
| Rate Limit | Enter the rate in milliseconds at which the MSE generates notifications. A value of 0 (default) means that the MSE generates notifications as fast as possible (Northbound notifications only). |
| Queue Limit | Enter the event queue limit for sending notifications. The MSE drops any event preceding this limit. |
| Retry Count | Enter the number of times to generate an event notification before the refresh time expires. This field can be used for asynchronous transport types which do not acknowledge the receipt of the notification and there is a possibility that the notification might be lost in transit. Default value is 1.<br>**Note** The MSE does not store events in its database. |

| Field | Configuration Options |
|---|---|
| Refresh Time | Enter the wait time, in minutes, that must pass before a notification is resent. For example if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. |
| Drop Oldest Entry on Queue Overflow | (Read-only). The number of event notifications dropped from the queue since startup. |
| Serialize Events per Mac address per Destination | Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner. |

# Field Reference for MSE Alarm Detail Page

The following table describes the fields in MSE Alarm detail page.

***Table 6: MSE Alarm Details***

| | |
|---|---|
| Failure Source | The MSE that generated the alarm. |
| Owner | Name of person to which this alarm is assigned, or blank. |
| Acknowledged | Displays whether or not the alarm is acknowledged by the user. |
| Category | The category of the alarm.The Alarm category is Mobility Services for MSEs. |
| Created | Month, day, year, hour, minute, second, AM or PM alarm created. |
| Modified | Month, day, year, hour, minute, second, AM or PM alarm last modified. |
| Failure Source | The MSE that generated the alarm. |
| Generated By | This field displays MSE. |
| Failure Source | The MSE that generated the alarm. |

The General information might vary depending on the type of alarm. For example, some alarm details might include location and switch port tracing information.

- Related Alarm List—Displays all the alarms related to a particular attack.
- Rogue Client Details—Displays information about the rogue clients.
- Annotations—Enter any new notes in this text box and click **Add** to update the alarm. Notes appear in the “Annotations” display page.
- Messages—Displays information about the alarm.
- Device Details
- Switch Port Tracing
- Location Notification
- Map Location

- Device Events
- Related History
- Audit Report—Click to view config audit alarm details. This report is only available for Config Audit alarms.

Configuration audit alarms are generated when audit discrepancies are enforced on config groups. If enforcement fails, a critical alarm is generated on the config group. If enforcement succeeds, a minor alarm is generated on the config group. The alarms have links to the audit report where you can view a list of discrepancies for each controller.

- Event History—Opens the MSE Alarm Events page to view events for this alarm. When there are multiple alarm pages, the page numbers appear at the top of the page with a scroll arrow on each side. Use these scroll arrows to view additional alarms.

# Field Reference for MSE Clients Page

The following table describes the fields in MSE Clients page.

***Table 7: MSE Clients Details***

| Field | Descriptions |
|---|---|
| MAC Address | Client MAC address. |

| Field | Descriptions |
|---|---|
| IP Address | Client IP address.<br>The IP Address that appears in the IP Address column is determined by a predefined priority order. The first IP address available in the following order appears in the IP address text box:<br>• IPv4 address<br>**Note** Only wireless clients have IPv6 addresses in this release. Each client can have up to 16 IPv6 addresses and 4 IPv4 addresses.<br>• IPv6 global unique address. If there are multiple addresses of this type, most recent IPv6 address that the client received is shown, because a user could have two Global IPv6 addresses but one might have been from an older Router Advertisement that is being aged out.<br>• IPv6 local unique address. If there are multiple IPv6 local unique addresses, then the most recent address appears.<br>• IPv6 link local address. For an IPv6 client it always have at least a link local address.<br>• The following are the different IPv6 address types:<br>• Link-local Unicast—The link-local addresses are designed to be used for addressing on a single link for purposes such as auto-address configuration, neighbor discovery, or when no routers are present.<br>• Site-local Unicast—The site-local addresses are designed to be used for addressing inside of a site without the need for a global prefix.<br>• Aggregatable Global Unicast—The aggregatable global unicast address uniquely identifies the client in global network and equivalent to public IPv4 address. A client can have multiple aggregatable global unicast addresses. |
| IP Type | The IP address type can be IPv4 and IPv6.<br>• Global Unique<br>• Unique Local<br>• Link Local |
| Refresh Time | Enter the wait time, in minutes, that must pass before a notification is resent. For example if a device is configured for In Coverage Area notification and it is constantly being detected within the Coverage Area. The notification is sent once every refresh time. |
| Drop Oldest Entry on Queue Overflow | (Read-only). The number of event notifications dropped from the queue since startup. |
| Serialize Events per Mac address per Destination | Select this option if you want the successive events for the same MAC address to be sent to a single destination in a serial manner. |
| User Name | Username based on 802.1x authentication. Unknown is displayed for client connected without a username. |
| Type | Indicates the client type. |

| Field | Descriptions |
|---|---|
| Vendor | Device vendor derived from OUI. |
| Device Name | Network authentication device name. For example, WLC and switch. |
| Location | Map location of the connected device. |
| VLAN | Indicates the access VLAN ID for this client. |
| Status | Current client status.<br>• Idle—Normal operation; no rejection of client association requests.<br>• Auth Pending—Completing a AAA transaction.<br>• Authenticated—802.11 authenticated complete.<br>• Associated—802.11 association complete. This is also used by wired clients to represent that a client is currently connected to the network.<br>• Disassociated—802.11 disassociation complete. This is also used by wired clients to represent that a client is currently not on the network.<br>• To Be Deleted—The client is deleted after disassociation.<br>• Excluded—Automatically disabled by the system due to perceived security threat. |
| Interface | Controller interface (wireless) or switch interface (wired) that the client is connected to. |
| Protocol | • 802.11—wireless<br>• 802.3—wired |
| Association Time | Last association start time (for wireless client). For a wired client, this is the time when a client is connected to a switch port. This is blank for a client which is associated but has problems being on the network. |
| CCX | Lightweight wireless only. |

# Field Reference: Context Aware Partner and Tag Engine Status for MSE

The following table describes the fields in the Tag Engine Status page for the Aeroscout Tag Engine.

***Table 8: Partner Engine Status Fields***

| Field | Description |
|---|---|
| Partner Location Engine Name | The Partner engine name, which is **aeroscout**. |
| Version | Version of the Aeroscout Tag Engine. |
| Description | Description for the Tag Engine. |

| Field | Description |
|---|---|
| Registered | Appears as True when the Aeroscout Tag Engine has established communication with the MSE. |
| Active | Appears as True when the Aeroscout Tag Engine is up and running. |
| License Information | The maximum tags that are available with the Aeroscout Tag Engine. |

If you selected Cisco Tag Engine for Context Aware Service, the Tag Engine Status page displays the following information.

The following table describes the fields in the Tag Engine Status page for the Cisco Tag Engine.

***Table 9: Tag Engine Status Fields***

| Field | Description |
|---|---|
| Tag Location Engine Name | The Tag location engine name, which is **Cisco**. |
| Version | Version of the Cisco Tag Engine. |
| Description | Description for the Cisco Tag Engine. |
| Active | Displays as True when the Cisco Tag Engine is up and running. |
| License Information | The maximum tags that are available with the Cisco Tag Engine. |

# Field Reference: Converged Access Templates

This section contains the field descriptions for converged access template.

***Table 10: Wireless Management Field Descriptions***

| Field Name | Description |
|---|---|
| VLAN ID | VLAN ID of the selected device. |
| IP Address | Wireless management IP of the selected device. |
| Subnet mask | Subnet mask allocated to the selected device. |

***Table 11: WLAN Field Descriptions***

| Field | Description |
|---|---|
| SSID | Name of the wireless LAN. |
| ID | Wireless LAN ID. If SSID > 16, you need to manually enter the AP group name. |

| Field | Description |
|---|---|
| Security | Allows you to customize the login window for configuring an external web server such as ISE. The following security options are available for WLAN:<br>• WPA2-Enterprise<br>• WPA2-Personal<br>• OPEN<br>For Guest WLAN, WebAuth (external) option alone is available. |
| Pre-Shred Key | This is a mandatory field, if you have a selected WPA2-Personal. The value must be alphanumeric and at least eight characters long. |
| Client VLAN Name | Name of the client VLAN. Can be alphanumeric. |
| AP Group | AP Group name is used to assign group name for the APs associated with WLAN and Client VLAN. |
| DHCP Required | This is an optional field. Check the **DHCP Required** check box for WLAN. This forces the wireless clients to use DHCP to get IP addresses. Clients with static address cannot access the network. |
| Radio | Radio bands used by WLAN. |
| Device Classification | You can turn on/off the device classification on the switch, using OUI and DHCP. |
| Device Profiling | You can turn on/off the device profiling. The following two options are available for device profiling:<br>• Local profiling based on HTTP attributes<br>• Radius profiling based on HTTP attributes |
| Client Exclusion | Turns on/off the client exclusion for the WLAN. When it is turned on, the misbehaving clients are added in an exclusion list so that they cannot access the network until the timeout is over. Clients may be added in the exclusion list due to excessive authentication attempts and using IP address of another client. |
| Client Exclusion Timeout (sec) | The timeout period for excluded clients. |
| Session Timeout (sec) | The timeout period for a client session. The client is re-authenticated before this period is over. |

***Table 12: Wireless Radio Field Descriptions***

| Field | Description |
|---|---|
| RF Group Name | Name of the RF group. Multiple MCs can be placed under a single RF group, to perform RRM in a globally optimized manner and perform network calculations on a per-radio basis. |
| Radio 2 GHz | This is an optional check box. |
| Radio 5 GHz | This check box is checked by default and it’s mandatory. You cannot uncheck this check box |
| Disable Rates | These data rates are disabled. Clients cannot use these data rates to connect to access points. |

| Field | Description |
|---|---|
| Mandatory Rates | Clients must support these data rates in order to associate to an access point, although it may connect to the AP using one of the supported data rates. |
| Supported Rates | Clients that support this data rate may communicate with the access using the supported date rate. However, clients are not required to use this data rate in order to associate with the AP. |
| Country Code | Country code enables you to specify a particular country of operation. Configuring a country code ensures that each radio's broadcast frequency bands, interfaces, channels, and transmit power levels are compliant with country-specific regulation. |

***Table 13: Guest Services Field Descriptions***

| Field | Description |
|---|---|
| Anchor Controller IP | Wireless management IP of Guest Anchor device. |
| Anchor Group Name | Group name of Anchor device. |
| Foreign Controller | Wireless management IP of MC to which the Guest Anchor device is associated. |

Refer the table WLAN Field Descriptions for reference.

***Table 14: Security Field Descriptions***

| Field | Description |
|---|---|
| Radius Server (IPs) | IP address of the Remote Authentication Dial In User Service (RADIUS) server. |
| Key | Password of Radius server. |
| Device HTTP TACACS Authentication | Select this in order to enable TACACS based device authentication to access the converged access device. |
| TACACS+ Server IP(s) | IP address of the TACACS server. |
| Key | Password of the TACACS server. |

***Table 15: Application Services Field Descriptions***

| Field Name | Description |
|---|---|
| Netflow Collectors (IP:Port) | IP—The IP address of the Prime Infrastructure server.<br>Port—The port on which the NetFlow monitor will receive the exported data. For Cisco Prime Infrastructure the default port is 9991.<br>Example: 172.20.114.251:9991 |
| WLAN-1 SSID Bandwidth(%) | Specify the maximum bandwidth percentage allowed for first WLAN. |
| WLAN-2 SSID Bandwidth(%) | Specify the maximum bandwidth percentage allowed for second WLAN. |

| Field Name | Description |
|---|---|
| WLAN-3 SSID Bandwidth(%) | Specify the maximum bandwidth percentage allowed for third WLAN. |
| Guest SSID Bandwidth(%) | Specify the maximum bandwidth percentage allowed for Guest WLAN. |

*Table 16: Wireless Mobility Field Descriptions*

| Field Name | Description |
|---|---|
| Role | Mobility Controller or Mobility Agent. |
| Controller IP | Wireless Management IP of Controller device. |
| Switch Peer Group Name | Peer group name in which the Agent is added. |
| Mobility Agent IP(s) | Wireless management IP of Mobility Agent devices. If you are entering more than one IP addresses, use semicolon to separate the IP addresses. |
| Peer Controller IP(s) | Wireless Management IP of peer controller device. If you are entering more than one IP addresses, use semicolon to separate the IP addresses. |

# Mobility Services Field Descriptions

The following topics contain field descriptions for designing the mobility services engine:

- Mobility Services
- Mobility Services
- MSE High Availability

## Mobility Services

The following table shows the field description in **Services > Mobility Services > Spectrum Experts** page.

*Table 17: Field Descriptions in Spectrum Experts page*

| Field | Description |
|---|---|
| Hostname | Displays the host name or IP address. |
| Active Interferers | Indicates the current number of interferes being detected by the Spectrum Experts. |
| Alarms APs | The number of access points seen by the Spectrum Experts that are potentially affected by detected interferers. |
| Alarms | The number of active interference traps sent by the Spectrum Expert. Click to access the Alarm page that is filtered to the active alarms for this Spectrum Expert. |

| Field | Description |
|---|---|
| Reachability Status | Indicates “Reachable” in green if the Spectrum Expert is running and sending data to Prime Infrastructure. Otherwise, indicates “unreachable” in red. |
| Location | When the Spectrum Expert is a wireless client, a link for location is available. It shows the location of the Spectrum Expert with a red box that shows the effective range. |
| Interferer ID | An identifier that is unique across different spectrum experts. This is a pseudo-randomly generated ID. Though it is similar to a MAC address, it is not a real address, which you can use to find the interfering device. |
| Category | Indicates the category of the interferer. Categories include: Bluetooth, cordless phones, microwave ovens, 802.11 FH, generic: fixed-frequency, jammers, generic: frequency-hopped, generic:continuous, and analog video. |
| Type | Active indicates that the interferer is currently being detected by a spectrum expert. Inactive indicates that the interferer is no longer detected by a spectrum expert or the spectrum expert saw that the interferer is no longer reachable by Prime Infrastructure. |
| Discover Time | Indicates when the interferer was discovered. |
| Affected Channels | Identifies affected channels. |
| Number of APs Affected | The number of access points managed by Prime Infrastructure that the spectrum expert detects or the interferers that the spectrum expert detected on the channels of the access point. Only active interferers are shown. If all of the following conditions are met, the access point is labelled as affected:If the access point is managed by Prime Infrastructure.If the spectrum expects detects the access point.If the spectrum expert detects an interferer on the serving channel of the access point. |
| Power | Indicated in dBm. |
| Duty Cycle | Indicated in percentage. 100% is the worst value. |
| Severity | Indicates the severity ranking of the interferer. 100 is the worst case whereas 0 is no interference. |
| Total Interferer Count | Given from the specific spectrum expert. |
| Active Interferers Count Chart | Displays a pie chart that groups interferers by category. |
| Active Interferer Count Per Channel | Displays the number of interferers grouped by category on different channels. |
| AP List | Provides a list of access points detected by the spectrum expert. These access points are on channels that have active interferers detected. |
| Affected Clients List | Provides a list of clients that are currently authenticated to an access point. You can select specific RADIUS or LDAP servers to provide external authentication in the Security > AAA page. |

# Mobility Services Engines

The following sections contain field description for pages found in **Design > Mobility Services > Mobility Services Engine**.

- **Mobility Services Engines > Select a command > Add Mobility Services Engine**

## Mobility Services Engines Select a command Add Mobility Services Engine

The following table describes the Template Detail fields in **Design > Mobility Services > Mobility Services Engine > Select a command > Add a Mobility Services Engine**.

***Table 18: Add Mobility Services Engine***

| Field | Description |
|---|---|
| Device Name | User-assigned name for the mobility services engine. |
| IP Address | The IP address of the mobility service engine. |
| Contact Name | The mobility services engine administrator. |
| Username | The default username is admin. This is the Prime Infrastructure communication username configured for MSE. |
| Password | The default password is admin. This is the Prime Infrastructure communication password configured for MSE. |

# MSE High Availability

The following table describes the Template Detail fields in **Services > Mobility Services > MSE High Availability**.

***Table 19: Configure High Availability***

| Field | Description |
|---|---|
| Device Name | Secondary device name with which you want to pair the primary MSE. |
| IP Address | Secondary IP address which is the health monitor IP address of the secondary MSE. |
| Failover Type | Specify the failover type. You can choose either Manual or Automatic. After 10 seconds, the system fails over. The secondary server waits for a maximum of 10 seconds for the next heartbeat from the primary server. If it does not get the heartbeat in 10 seconds, it declares a failure. |
| Failback Type | Specify the failback type. It can be either Manual or Automatic. |
| Long Failover Wait | Specify the long failover wait in seconds. After 10 seconds, the system fails over. The maximum failover wait is 2 seconds. |
| Secondary password | The password configured in the Secondary MSE. |
| Secondary Platform UDI ->Browse -> Click Activate | To activate MSE HA, apply permanent or evaluation license for Secondary UDI. |

# Connected Mobile Experiences

The following table describes the Template Data fields in the following:

- **Services > Mobility Services > Connected Mobile Experiences**.
- **Services > Mobility Services > Mobility Services Engines > Click Here to manage CMX**

*Table 20: Connected Mobile Experiences*

| Field | Description |
|---|---|
| IP Address | The IP address of the CMX. |
| Device Name | User-assigned name for the CMX. |
| User Name | The default username is admin. This is the Prime Infrastructure communication username configured for CMX. |
| Password | The default password is admin. This is the Prime Infrastructure communication password configured for CMX. |
| Owner (optional) | Specify the user assigned unique value for CMX. |