{

// specify a time zone if the timestamps in your log are not in GMT

// timezone: "GMT-0800"

attributes: {

"metadata.product.name": "Unifi Networks",

"metadata.product.vendor\_name": "Ubiquiti",

"dataSource.category": "security",

"dataSource.name": "Unifi Networks",

"dataSource.vendor": "Ubiquiti"

},

patterns: {

timestamp: "([a-z]+\\s+[0-9]+\\s+[0-9:]+)|" // e.g. Feb 3 03:47:01

+ "(\\d{4}-\\d{2}-\\d+T\\d{2}:\\d{2}:\\d{2}.\\d+\\+\\d+:\\d{2})" // e.g. 2013-03-20T00:53:26.942569+00:00

},

formats: [

{

format: "$timestamp=timestamp$ $device\_host$ $device\_mac\_addr$,$metadata.product.version$: $process$: \\[$procid$\\] $syslog\_msg$",

halt: true

}, {

format: "$timestamp=timestamp$ $device\_host$ $device\_mac\_addr$,$metadata.product.version$: $process$\\[$procid$\\]: $syslog\_msg$",

halt: true

}, {

format: "$timestamp=timestamp$ $device\_host$ \\{$device\_serial\_number$\\} \\[$procid$\\] $syslog\_msg$",

halt: true

},

]

}