{

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

// timezone: "America/Chicago"

attributes: {

"dataSource.category": "security",

"dataSource.name": "Managed Engine",

"dataSource.vendor": "Managed Engine",

"metadata.product.vendor\_name": "Managed Engine",

},

patterns: {

tzPattern: "(\\w{3} \\d{1,2} \\d{2}:\\d{2}:\\d{2})",

ipPattern: "((\\d+\\.){3}\\d+|[a-zA-Z0-9:]+)", // Extract IPv4 or IPv6 addresses

},

formats: [

{

id: "ADSSP",

format: "\\<\\d+\\>$timestamp=tzPattern$ $hostname$ $metadata.product.name$: "

}, {

id: "ADAuditPlus",

format: "\\<\\d+\\>\\d $timestamp$ $hostname$ $metadata.product.name$ - - -"

}, {

format: ".\*\\[$\_=identifier$=$\_$\\]",

repeat: true

},

]

}