



## Service Description: Cisco Intrusion Prevention System (IPS) Signature Management Service

This document describes the Cisco Intrusion Prevention System (IPS) Signature Management Service.

**Related Documents:** The following documents posted at [www.cisco.com/go/servicedescriptions/](http://www.cisco.com/go/servicedescriptions/) should be read in conjunction with this Service Description and are incorporated into this Service Description by this reference: (1) ROS Supported-Device List (which identifies the devices that are supported under Cisco IPS Signature Management Service), (2) ROS Glossary of Terms, (3) List of Services Not Covered, and (4) Severity and Escalation Guidelines.

**Direct Sale from Cisco.** If you have purchased these Services directly from Cisco, this document is incorporated into your Master Services Agreement (MSA) or equivalent services agreement executed between you and Cisco. All capitalized terms not defined in the Supplemental Glossary of Terms at the end of this document have the meanings ascribed in the MSA.

**Sale via Cisco Authorized Reseller.** If you have purchased these Services through a Cisco Authorized Channel, this document is for description purposes only; it is not a contract between you and Cisco. The contract, if any, governing the provision of this Service will be the one between you and your Cisco Authorized Channel. Your Cisco Authorized Channel should provide this document to you, or you can obtain a copy of this and other Cisco service descriptions at [www.cisco.com/go/servicedescriptions/](http://www.cisco.com/go/servicedescriptions/). All capitalized terms not defined in the Supplemental Glossary of Terms at the end of this document have the meanings ascribed in the ROS Glossary of Terms (or Cisco's standard Glossary of Terms, if applicable) posted at the above URL.

### Cisco IPS Signature Management Service

The Cisco Intrusion Prevention System (IPS) Signature Management Service consists of processes used by the Cisco NOC to manage the Cisco Secure Intrusion Prevention System (IPS) configuration, as limited by the approved device and Managed Component list. In addition, the Service includes IPS specific notifications.

#### Cisco Responsibilities:

- Remote Release Management Activities. Cisco will:

Upon release of new signature pack update, distribute and upgrade new Cisco Secure IPS operating system and signature releases to applicable Managed Components. Distribution of each new release is a Standard Change. Distribution of new releases may take place during the weekly Change Management Window. If Customer and Cisco have not agreed to a Change Management Window, distribution of a new release may occur at any time in Cisco's discretion within the first 24 hours of official public availability of the applicable release.

- Remote Signature Tuning Activities. Cisco will:

Review applicable alarm activity associated with the Cisco Secure IPS within the Managed Components for evidence of repetitive benign event triggers, within two weeks following distribution of each Cisco IPS signature release.

Implement filters for benign triggers in the configuration of the Cisco Secure IPS within the Managed Components to reduce benign alarms, where determined necessary in the sole opinion of Cisco. Implementation of filters by Cisco is a Standard Change, and may be done by Cisco at any time during the term of the Service.

- Notification Activities. Cisco will:

Notify Customer, via email, within four (4) hours of the completion of Remote Release Management Activities (as described above) associated with a release.

Notify Customer, via email, within four (4) hours of the completion of any Remote Signature Tuning Activities (as described above).

### **Customer Responsibilities**

Customer will supply to Cisco and/or the applicable Authorized Channel the information, communications, and connectivity as described below within ninety (90) days of the applicable Purchase Order for the Services.

- Connectivity and Access to Managed Components. Customer will:
  - Provide Secure Shell (SSH) access from Cisco to the management interface of the Managed Component.
  - Provide Secure Socket Layer (SSL) access from Cisco to the management interface of the Managed Component.
  - Ensure that the Cisco IPS Signature Management Service network ranges, provided during Service Activation, are added to the allowed hosts within the configuration of the Managed Component.
- Notification of Changes. Customer will inform Cisco in writing of any changes that affect Cisco connectivity and access to Managed Components, before they take place.
- Weekly Change Management Window. Customer may propose a range of times for a weekly Change Management window. All Change Management windows are subject to approval by Cisco and/or the applicable Authorized Channel, as applicable.
- Additional Services Not Covered. In addition to the List of Services Not Covered posted at [www.cisco.com/go/servicedescriptions/](http://www.cisco.com/go/servicedescriptions/), the following are not supported or provided under the Cisco IPS Signature Management Service:
  - Support of any device, item or other equipment (including any Managed Component) that is not managed by a Service.
  - Cisco, in its discretion, reserves the right to not provide Services on any particular Managed Component as identified and communicated during Service Activation (e.g., if the Managed Component is not serviceable, etc.)

**Supplemental Glossary of Terms for  
Cisco Intrusion Prevention System (IPS) Signature Management Service**

**Supplemental Glossary of Terms**

"Standard Change" means a change to IT resources which follows an established path, is relatively common for Cisco, and is an accepted solution to a specific requirement (or set of requirements), in each case as reasonably determined by Cisco in connection with Service Activation or thereafter (or as otherwise mutually agreed upon by Cisco and Customer in writing). Cisco may make Standard Changes without any prior approval of Customer.

"Change Management Window" means a pre-determined, recurring time period during which Cisco may implement change(s) on Managed Components, as reasonably determined by Cisco in connection Service Activation or thereafter (or as otherwise mutually agreed upon by Cisco and Customer in writing).

"Service Activation" is a process in which Cisco prepares and activates an Intrusion Prevention System (IPS) for the Cisco IPS Signature Management Service. During this process, Cisco and the Customer will agree on co-management responsibilities for the entitled IPS appliance or module. The Service Activation process begins on the date of Cisco's acceptance of a Purchase Order for Service, and ends no more than ninety (90) days later.