

ALIBABA CLOUD

阿里云

Web应用防火墙
安全服务

文档版本：20200910

 阿里云

法律声明

阿里云提醒您在阅读或使用本文档之前仔细阅读、充分理解本法律声明各条款的内容。如果您阅读或使用本文档，您的阅读或使用行为将被视为对本声明全部内容的认可。

1. 您应当通过阿里云网站或阿里云提供的其他授权通道下载、获取本文档，且仅能用于自身的合法合规的业务活动。本文档的内容视为阿里云的保密信息，您应当严格遵守保密义务；未经阿里云事先书面同意，您不得向任何第三方披露本手册内容或提供给任何第三方使用。
2. 未经阿里云事先书面许可，任何单位、公司或个人不得擅自摘抄、翻译、复制本文档内容的部分或全部，不得以任何方式或途径进行传播和宣传。
3. 由于产品版本升级、调整或其他原因，本文档内容有可能变更。阿里云保留在没有任何通知或者提示下对本文档的内容进行修改的权利，并在阿里云授权通道中不时发布更新后的用户文档。您应当实时关注用户文档的版本变更并通过阿里云授权渠道下载、获取最新版的用户文档。
4. 本文档仅作为用户使用阿里云产品及服务的参考性指引，阿里云以产品及服务的“现状”、“有缺陷”和“当前功能”的状态提供本文档。阿里云在现有技术的基础上尽最大努力提供相应的介绍及操作指引，但阿里云在此明确声明对本文档内容的准确性、完整性、适用性、可靠性等不作任何明示或暗示的保证。任何单位、公司或个人因为下载、使用或信赖本文档而发生任何差错或经济损失的，阿里云不承担任何法律责任。在任何情况下，阿里云均不对任何间接性、后果性、惩戒性、偶然性、特殊性或刑罚性的损害，包括用户使用或信赖本文档而遭受的利润损失，承担责任（即使阿里云已被告知该等损失的可能性）。
5. 阿里云网站上所有内容，包括但不限于著作、产品、图片、档案、资讯、资料、网站架构、网站画面的安排、网页设计，均由阿里云和/或其关联公司依法拥有其知识产权，包括但不限于商标权、专利权、著作权、商业秘密等。非经阿里云和/或其关联公司书面同意，任何人不得擅自使用、修改、复制、公开传播、改变、散布、发行或公开发表阿里云网站、产品程序或内容。此外，未经阿里云事先书面同意，任何人不得为了任何营销、广告、促销或其他目的使用、公布或复制阿里云的名称（包括但不限于单独为或以组合形式包含“阿里云”、“Aliyun”、“万网”等阿里云和/或其关联公司品牌，上述品牌的附属标志及图案或任何类似公司名称、商号、商标、产品或服务名称、域名、图案标示、标志、标识或通过特定描述使第三方能够识别阿里云和/或其关联公司）。
6. 如若发现本文档存在任何错误，请与阿里云取得直接联系。

通用约定

格式	说明	样例
 危险	该类警示信息将导致系统重大变更甚至故障，或者导致人身伤害等结果。	 危险 重置操作将丢失用户配置数据。
 警告	该类警示信息可能会导致系统重大变更甚至故障，或者导致人身伤害等结果。	 警告 重启操作将导致业务中断，恢复业务时间约十分钟。
 注意	用于警示信息、补充说明等，是用户必须了解的内容。	 注意 权重设置为0，该服务器不会再接受新请求。
 说明	用于补充说明、最佳实践、窍门等，不是用户必须了解的内容。	 说明 您也可以通过按Ctrl+A选中全部文件。
>	多级菜单递进。	单击设置> 网络> 设置网络类型。
粗体	表示按键、菜单、页面名称等UI元素。	在结果确认页面，单击确定。
<code>Courier</code> 字体	命令或代码。	执行 <code>cd /d C:/window</code> 命令，进入Windows系统文件夹。
<i>斜体</i>	表示参数、变量。	<code>bae log list --instanceid</code> <i>Instance_ID</i>
[] 或者 [a b]	表示可选项，至多选择一个。	<code>ipconfig [-all -t]</code>
{ } 或者 {a b}	表示必选项，至多选择一个。	<code>switch {active stand}</code>

目录


1.概述	05
2.安全专家指导服务	06
3.WAF产品专家服务	09
4.WAF产品托管服务	11
5.产品托管服务授权	13
6.开通WAF安全服务授权	14
7.查看安全专家操作日志	16
8.取消WAF安全服务授权	18

1.概述

安全服务帮助您解决Web应用防火墙使用过程中遇到的问题，协助您完成网站接入、防护配置、安全分析等任务。

根据服务形式和计费方式的不同，Web应用防火墙提供以下安全服务。

名称	描述	是否收费	适用场景或对象	交付方式	开通方式
安全专家指导服务	您可以加入阿里云企业安全服务钉钉群或者创建企业专属的安全服务钉钉群，免费享受安全专家通过钉钉为您提供的一对一指导服务，解决产品使用过程中遇到的困难或紧急问题。	否	日常咨询	安全服务钉钉群或者企业专属钉钉群	开通Web应用防火墙后，通过控制台加入安全服务钉钉群。
WAF产品专家服务	您可以通过预付费方式开通WAF产品专家服务，享受阿里云认证合作伙伴提供的Web应用防火墙技术支持，包括安全咨询、产品接入配置、策略定制、日常巡检与监控、应急响应等。	是	中国内地的中小型企业、个人用户	企业专属钉钉群	开通Web应用防火墙包年包月服务时，在购买页选择开启产品专家服务。
WAF产品托管服务	您可以通过预付费方式开通WAF产品托管服务，享受阿里云原厂安全服务团队提供的全面的Web应用防火墙技术支持，例如接入设置、防护策略优化、监控与告警设置、安全报表定制等。 使用该服务时，您需要开通服务授权，允许阿里云安全服务专家查看您的业务场景数据，以便提供有针对性的防护咨询和日志数据深度分析建议。更多信息，请参见 开通WAF安全服务授权 。	是	需要外包专业人员协助进行安全产品服务运营的用户、企业级用户、国际用户	企业专属钉钉群、电话会议、邮件等	在WAF产品托管服务售卖页购买。

 **说明** 关于钉钉聊天应用，请参见[阿里云钉钉官网首页](#)。

2.安全专家指导服务

阿里云Web应用防火墙支持通过钉钉服务群为您提供免费的一对一专家指导服务。您在使用Web应用防火墙过程中遇到任何问题时，都可以通过Web应用防火墙管理控制台的专家指导服务入口获取7*24的Web应用防火墙产品帮助服务。

前提条件

- 已经开通过Web应用防火墙服务。更多信息，请参见[开通Web应用防火墙](#)。
- 已经在手机移动端安装并注册使用钉钉聊天应用。更多信息，请参见[阿里巴巴钉钉官网](#)。

背景信息

安全专家指导服务支持以下两种方式：

- **加入阿里云官方钉钉服务群咨询问题**：适合咨询相对简单的问题，加入临时的官方产品服务群，不需要多个业务相关人员参与提问。
- **创建并使用企业专属钉钉服务群咨询问题**：适合企业级用户，可以创建7*24的专属服务群，随时咨询产品使用过程中的任何问题，支持邀请多个企业业务相关人员共同参与提问。


加入阿里云官方钉钉服务群咨询问题

1. 登录[Web应用防火墙控制台](#)。
2. 在左侧导航栏底部，单击有问题，找专家。

 **说明** 只有已经开通过Web应用防火墙服务后，才会显示有问题，找专家。

3. 打开手机钉钉应用，扫描显示的二维码，申请加入WAF紧急事件处理群。
成功加入WAF紧急事件处理群后，您可以在群里直接咨询使用Web应用防火墙时遇到的问题。钉钉群内的安全专家将通过钉钉为您提供一对一指导服务，帮助您妥善解决Web应用防火墙产品使用过程中遇到的任何问题。

创建并使用企业专属钉钉服务群咨询问题

 **说明** 目前该入口仅向2020年6月后首次开通Web应用防火墙服务的用户开放。如果您在2020年6月之前已经开通过Web应用防火墙服务，则不支持通过Web应用防火墙控制台创建企业专属钉钉服务群，建议您通过阿里云官方钉钉服务群联系我们帮助您创建专属钉钉服务群。更多信息，请参见[加入阿里云官方钉钉服务群咨询问题](#)。

1. 登录[Web应用防火墙控制台](#)。
2. 在左侧导航栏底部，单击有问题，找专家。

 **说明** 只有已经开通过Web应用防火墙服务后，才会显示有问题，找专家。

3. 创建企业专属钉钉服务群。
 - i. 单击使用钉钉注册手机号。

 **说明** 只有在2020年6月后首次开通Web应用防火墙服务，才会显示使用钉钉注册手机号。

ii. 填写企业专属钉钉服务群的注册信息。

加入你的钉钉专属群 ×

📄 使用钉钉扫描二维码咨询使用方法

📞 使用钉钉注册手机号

钉钉注册手机号

钉钉昵称

企业名称

提交

参数	说明
钉钉注册手机号	填写成功注册了钉钉应用的中国手机号码。
钉钉昵称	填写使用当前手机号码注册的钉钉名称。
企业名称	填写您的公司简称。示例：阿里云。

iii. 单击提交。

提交申请后，钉钉会立即为您创建专属的阿里云企业安全服务群，群名称默认为“【安全】企业名称企业服务群”。

🔍 说明 如果您收到申请建群失败的提示，建议您通过扫描二维码的方式联系我们，安全专家收到您的问题后将会第一时间与您沟通。更多信息，请参见[加入阿里云官方钉钉服务群咨询问题](#)。

成功创建并加入阿里云企业安全服务群后，您可以在群里直接咨询使用Web应用防火墙时遇到的问题。钉钉群内的安全专家将通过钉钉为您提供一对一指导服务，帮助您快速解决Web应用防火墙产品使用过程中遇到的任何问题。

4. （可选）邀请企业中其他业务相关业务人员加入企业专属安全服务群。

i. 单击使用钉钉注册手机号。

ii. 填写要加入企业专属安全服务群的钉钉用户的信息。



参数	说明
钉钉注册手机号	填写成功注册了钉钉应用的中国手机号码。
钉钉昵称	填写使用当前手机号码注册的钉钉名称。

iii. 单击提交。


提交申请后，您申请的钉钉用户将自动加入到企业专属安全服务群，并可以在群内直接提问。

3.WAF产品专家服务

Web应用防火墙包年包月服务提供产品专家增值服务。您只需在开通WAF实例时选择开启产品专家服务，即可在WAF实例的有效期内享受阿里云技术工程师通过钉钉群向您提供的5*8技术支持服务，具体包括安全咨询、产品接入配置、策略定制、日常巡检与监控、应急响应等。

功能特性

下表描述了WAF产品专家服务与WAF产品托管服务的功能点差异。

 说明 关于WAF托管服务的更多信息，请参见[WAF产品托管服务](#)。

图标说明：√表示支持，×表示不支持，○表示增值（即需要单独购买）。

类别	对比项	产品专家服务	WAF托管服务
服务定位	服务对象	中国内地的中小型企业、个人用户	企业级用户、国际用户
	服务方式	响应式服务	主动式服务
基本支持	阿里云原厂支持	×，由阿里云认证合作伙伴支持	√
	中文支持	√	√
	英文支持	×	√
安全咨询	WAF使用咨询	√	√
	Web攻防问题咨询	×	√
	业务风控策略咨询	×	√
接入配置	接入配置指导	√	√
	主动接入配置	×	√
	移动App接入支持	×	√
迁移服务	第三方WAF策略分析	×	○，需单独购买
	WAF策略迁移定制	×	○，需单独购买
	现场培训	×	○，需单独购买
策略定制	简单策略定制	√，只支持使用页面上的策略功能	√
	深度策略定制	×	√
	网络架构分析	×	√

类别	对比项	产品专家服务	WAF托管服务
	移动App防护策略	×	√
	研发优先支持	×	√
日常巡检与监控	主动安全巡检	×	√, 每天巡检
	IP黑洞监控	√	√
	攻击事件监控	×	√
	可用性异常监控	×	√
报表系统	报表系统	×	√
	报表定制	×	√
应急响应	安全攻防应急	√	√
	快速解除黑洞	×	√
	应急响应报告	×	√
沟通方式	钉钉群支持	√	√
	电话支持	×	√
	邮件支持	×	√
	每月电话会议沟通	×	√
服务SLA	服务时间	5*8	7*24

使用限制

产品专家服务仅对使用Web应用防火墙包年包月实例（高级版及以上套餐）的用户开放。

使用按量付费Web应用防火墙服务的用户暂不支持开启产品专家服务。

计费方式

产品专家服务根据您所购买的Web应用防火墙实例的时长按月计费，价格：2000元/月。

开通方式

- 通过包年包月方式开通Web应用防火墙实例时，您可以在Web应用防火墙购买页选择开启产品专家服务。
具体操作请参见[开通Web应用防火墙](#)。
- 已开通包年包月的Web应用防火墙实例后，您可以通过升级实例规格，在变配页面选择开启产品专家服务。
具体操作请参见[升级](#)。

4.WAF产品托管服务

云盾Web应用防火墙（WAF）支持产品托管服务。开通WAF产品托管后，您可以在阿里云安全产品专家的帮助下完成WAF接入配置、防护策略优化，并享有安全事件响应、安全咨询、安全培训与案例分享、安全报告分析等服务。

概述

WAF产品托管由阿里云原厂安全服务团队提供技术支持，面向云盾WAF用户提供产品托管服务。WAF产品托管帮助您更有效地使用WAF保护Web资产、降低业务安全风险、减少运维人力投入。

WAF产品托管适用于已开通阿里云Web应用防火墙，但缺乏业务持续监控能力和缺少可应对安全漏洞风险的安全工程师的业务场景。该服务适合需要外包专业人员协助来进行安全产品服务运营的用户。

说明 由于托管服务的部分工作内容（包括但不限于防护策略优化、监控和预警设置、安全报告定制等）需要使用WAF日志服务，如果您未购买WAF日志服务，上述托管服务可能存在无法交付的风险。建议您在选购WAF产品托管服务的同时，购买WAF日志服务功能。更多信息，请参见[开启WAF日志服务](#)。

服务内容

WAF安全托管为您提供完整的WAF接入和使用支持，下表描述了具体的服务内容。

服务类型	描述
接入配置	<ul style="list-style-type: none"> 在WAF上配置保护对象的域名策略。 协助用户配置和上传HTTPS证书（用户可自行上传）。 协助用户配置ECS和SLB的源站保护策略。 产品适配和访问测试验证。 用户保护域名变化时，调整相关配置。
防护策略优化	<ul style="list-style-type: none"> 在WAF上的业务出现异常时，提供诊断和排错服务。 基于攻防日志，优化用户安全防护策略和配置。 安全事件响应时，调整防护策略和提供方案，帮助用户缓解事件影响。 提供故障处理、CC防护规则、精准访问控制规则、数据风控等WAF防护配置建议。
监控和预警	<ul style="list-style-type: none"> 系统自动化监控WAF集群可用性故障。 系统自动化监控安全高危事件和攻击导致的异常事件。 人工在线判断和过滤监控事件预警。
安全报告	<ul style="list-style-type: none"> 根据用户要求提供定制化安全报告内容。 提供服务日报和服务月报，其中日报包括当天操作信息，月报包括操作数据和攻防数据分析。

安全事件响应时间

开通WAF安全托管后，当您遇到安全事件需要紧急协助时，服务团队响应您的时间遵循下表描述。

序号	优先级	定义	响应时间
1	危险	用户核心业务严重受损或完全不可用	15分钟
2	紧急	用户核心业务出现非全局异常	30分钟
3	高	用户非核心业务严重受损或不可用	2小时
4	中	用户非核心业务出现非全局异常	4小时
5	低	用户日常技术咨询	8小时


服务交付方式

下表描述了WAF产品托管的服务交付方式。

类别	描述
服务交付方式	远程在线服务
服务语言	中文和英语
服务周期	与用户购买周期一致
支持的服务渠道	<ul style="list-style-type: none">• 电子邮件• 钉钉• 电话

定价和售卖方式

WAF产品托管服务支持通过预付费方式开通，并且可按月或者按年续费。购买WAF产品托管服务，请前往[WAF产品托管服务售卖页](#)。

 **注意** 由于服务支持系统和服务人力资源投入的特殊性，WAF产品托管服务在支付购买后暂不支持退款。

5.产品托管服务授权

6. 开通WAF安全服务授权

通过WAF安全专家服务，您将获得阿里云安全服务专家和第三方安全专家为您提供的针对您业务场景的WAF产品安全服务，帮助您基于业务实际情况更好地使用WAF产品功能，保障您业务的网络应用安全。

背景信息


安全专家可以为您提供WAF中的域名接入咨询服务，同时通过对您的业务日志数据进行深度分析，有针对性地为您提供WAF防护配置的相关建议。

购买WAF产品安全服务后，您需要开通服务授权，阿里云安全服务专家和第三方安全专家才能通过阿里云安全服务平台为您提供产品服务。

 **说明** 您必须已购买或开通云盾Web应用防火墙产品，才能享受WAF安全专家服务。

操作步骤

1. 登录云盾先知（安全情报）管理控制台。
2. 定位到服务授权页面，您可以查看到您的WAF产品安全服务订单的授权情况。

 **说明** 一般情况下，新创建的安全服务订单状态为未授权。



服务名称	订单号	服务开始时间	服务状态	授权状态	操作
waf按量计费	201807271435747250075383	2018-07-27 14:35:23	服务中	未授权	查看授权协议 授权

3. 单击查看授权协议，确认并同意授权书内容后单击确定。

授权协议

授权书

致阿里云计算有限公司：

因我单位已订购贵司云盾安全产品，现我单位申请由阿里云云盾安全产品原厂服务人员和阿里云云盾第三方合作伙伴服务商为我单位提供云盾安全产品服务（具体服务类型见授权服务名称）。

为提供前述服务，我司同意阿里云和第三方合作伙伴服务商对我司云盾安全产品相关数据（包括但不限于用户使用统计数据、管理数据、设置数据、操作日志记录等）具有读写权限。用户使用统计数据包括但不限于产品总览、安全报表、全量日志等内容，管理数据包括但不限于产品配置列表、产品配置及管理、产品部分自定义功能详情查看等内容，设置数据包括但不限于产品功能与规格、产品和服务账单等内容，操作日志记录包括但不限于产品服务详情、订单、产品自定义策略配置的增、删、改日志记录和查看等内容。

上述云盾安全产品数据应仅限于云盾安全产品服务业务目的使用，未经我单位同意不得提供给其他任何第三方。

[确定](#)

4. 单击授权，跳转至服务订单所对应的云资源RAM角色授权页面，单击同意授权。

说明 为了确保与安全专家的交流，确认您已申请并开通与安全专家的专属钉钉服务群。

云资源访问授权

温馨提示：如需修改角色权限，请前往RAM控制台角色管理中设置，需要注意的是，错误的配置可能导致MSSP无法获取到必要的权限。

MSSP请求获取访问您云资源的权限

下方是系统创建的可供MSSP使用的角色，授权后，MSSP拥有对您云资源相应的访问权限。

AliyunMSSPAccessingWAFRole

描述：安全管家(MSSP)默认使用此角色来访问您在其他云产品中的资源

权限描述：用于安全管家服务角色的授权策略，包含WAF的部分权限

[同意授权](#) [取消](#)

授权完成后，在云盾先知（安全情报）管理控制台的服务授权页面，该服务订单的状态显示为已授权，您可以随时单击查看授权协议查看授权书。

同时，您的专属安全专家将通过阿里云安全服务平台直接查看您的WAF中相应的业务数据及配置数据，为您的业务提供专属的安全策略和建议。

说明 安全专家通过阿里云安全服务平台查看您WAF控制台进行的所有操作都将产生相应的操作日志，您可以随时登录阿里云控制台查看安全专家操作记录。

7.查看安全专家操作日志

安全专家通过阿里云安全服务平台查看您WAF控制台的所有操作都将产生相应的操作日志，您可以随时登录阿里云操作审计控制台查看相关操作记录，审计安全专家的操作行为。

操作步骤

1. 登录**操作审计管理控制台**，并选择**华东1（杭州）地域**。

说明 目前，所有WAF安全服务的操作日志记录均存储在华东1（杭州）地域的操作审计服务中。

2. 定位到**历史事件查询**页面，设置以下查询条件，查询您的专属安全专家在WAF控制台中的操作记录日志。

- **资源名称**：aliyunmsspaccessingwafrole
- **事件类型**：所有类型

说明 目前，WAF安全服务仅授权安全专家查看您WAF控制台中的数据，不具备更改配置等权限。因此，您也可以将事件类型条件设置为读类型，查询到的事件记录与选择所有事件类型得到的查询结果一致。

- **时间**：选择您想查询的时间范围。

说明 历史事件查询支持查看最近30天内的操作记录。



查询结果如下图所示。

事件时间	用户名	事件名称	资源类型
▶ [Redacted]	aliyunmsspaccessingwafrole:mssp	DescribeWebAttackTypePv	
▶ [Redacted]	aliyunmsspaccessingwafrole:mssp	DescribeWebAttackTypePv	
▶ [Redacted]	aliyunmsspaccessingwafrole:mssp	DescribeWebAttackTypePv	
▶ [Redacted]	aliyunmsspaccessingwafrole:mssp	DescribeWebAttackTypePv	
▶ [Redacted]	aliyunmsspaccessingwafrole:mssp	DescribeWebAttackTypePv	
▶ [Redacted]	aliyunmsspaccessingwafrole:mssp	DescribeWebAttackTypePv	
▶ [Redacted]	aliyunmsspaccessingwafrole:mssp	DescribeWebAttackTypePv	

3. 在事件列表中，单击操作记录可展开查看事件详情。

事件时间	用户名	事件名称	资源类型	资源名称	错误码
▶ [redacted]	root	DescribeRegions			
▼ [redacted]	aliyunmsspaccessingwafrole:mssp	DescribeWebAttackTypePv			
访问秘钥: [redacted]		事件源: [redacted]			
地域: cn-hangzhou		事件时间: [redacted]			
错误代码: [redacted]		请求ID: [redacted]			
事件ID: [redacted]		源IP地址: [redacted]			
事件名称: DescribeWebAttackTypePv		用户名: [redacted]			
相关资源					查看事件

4. 单击查看事件可查看该事件的详细参数。

8.取消WAF安全服务授权

WAF安全服务授权开通后，您可以随时在访问控制（RAM）控制台中删除WAF安全服务的授权角色，取消WAF安全服务授权。

操作步骤

1. 登录RAM控制台。
2. 定位到角色管理页面，找到授权服务订单时生成的MSSP安全产品服务的授权角色（AliyunMSSPAccessingWAFRole），单击删除。
3. 在删除角色对话框中，单击确定。
4. 获取并输入手机验证码，单击确定，通过手机验证。
授权角色删除成功后，在云盾先知（安全情报）管理控制台的服务授权页面中相应服务订单的状态将变更为未授权。

服务授权

开通授权后，阿里云安全服务专家和第三方安全专家通过阿里云安全服务平台为您提供云盾产品安全服务。
为了更好的交流，请确保您已申请开通了专属的钉钉群。若还没有专属的钉钉服务群，请钉钉扫码或者[点击申请建群](#)。
温馨提醒：申请入群时，请务必在“申请理由”里备注阿里云主账号UID。



服务名称	订单号	服务开始时间	服务状态	授权状态	操作
wa按量计费	201807271435747250075383	2018-07-27 14:35:23	服务中	未授权	查看授权协议 授权