

OSINT

LIVE CONNECTIONS VIEWER

开启深度检查的免费密钥 — 去哪里获取、如何添加、如何使用。

获取你的密钥

用户手册 · 2026年10月

777 SOFTWARE 免费 — 永远免费

1 — 为什么需要密钥？

OSINT 在你打开它的那一刻就能工作。面板会填满你的实时连接，已知恶意名单会与它们进行核对，每一行都会得到一个通俗的判定。你不需要任何密钥就能做到这一切，也没有需要创建的账户 — 无论是我们这里的，还是任何人那里的。

密钥增加的是深度。四个外部服务各自保存着关于互联网地址的不同种类的记忆 — 谁被举报过滥用、几十个扫描器怎么看、一个地址是否是互联网背景噪声的一部分、一个主机是否提供过恶意软件链接。每个服务都会给你一个免费的个人密钥 — 一小行秘密文本 — 当你把该密钥粘贴到 OSINT 中时，应用就可以以你的名义、用你的额度向该服务询问你面板上的地址。

本指南中的每一个密钥都是免费的，直接来自服务本身。如果某个页面曾经向你要卡，那你就是选错了套餐 — 关掉它，选择步骤中提到的免费套餐。

服务	它回答什么	需要密钥吗？
VirusTotal	有多少安全扫描器标记这个地址	是 — 免费密钥会开启它的按钮
AbuseIPDB	这个地址是否被举报过滥用，程度有多强	是 — 免费密钥会开启它（之后它会自己运行）
abuse.ch — URLhaus	这个主机是否提供过恶意软件链接	是 — 免费的 Auth-Key 会开启它的按钮
GreyNoise	互联网背景噪声，还是冲着你来的	否 — 无需密钥即可工作；密钥只会提高额度

你的密钥属于你。OSINT 把它们保存在你自己电脑上的一个设置文件中，并锁定为你的账户专用。它们从不上传，从不发送给 777 Software，也从不包含在任何下载中。当一项检查运行时，应用会把正在检查的地址 — 以及你的密钥 — 发送给该密钥自己的服务，不发送到其他任何地方。这就是全部安排，§ 6 会确切地告诉你这些密钥去了哪里。

2 — VIRUSTOTAL

它回答什么：几十个安全扫描器对一个地址投票。OSINT 会用通俗的话显示它们的计数 — 有多少说恶意、有多少说可疑、有多少说无害。

去哪里：virustotal.com

1. 在 VirusTotal 主页上，选择 Join us («加入我们») 开始创建一个免费账户。
2. 填写表格：你的名、姓、电子邮件地址、一个用户名和一个密码。（它们也提供 Google 登录 — 填写的表格效果相同。）
3. 通过 “I'm not a robot” («我不是机器人») 检查并提交表格。页面会回答 “Signed up successfully” («注册成功»)。
4. 打开它们发送给你的电子邮件，点击激活链接。没有这一次点击，账户会一直处于休眠状态。
5. 登录。打开你的个人资料菜单，选择 API key («API 密钥») 页面 — 你的个人密钥会显示在那里。
6. 复制完整的密钥。§ 6 会告诉你它在 OSINT 中应该放在哪里。

免费层级：一个标准的免费账户。API 密钥页面会这样说明，免费的公共额度是每天 500 次查询 — 远远超过一个人手工检查连接时可能用到的数量。

一条诚实的说明，秉承 VirusTotal 自己的精神：任何通过其 API 检查的地址都会被添加到 VirusTotal 数据集中，并可以被其社区看到。OSINT 在它的 Settings 中，VirusTotal 字段旁边，也说了同样的话。如果这个交换不适合你，就把该字段留空 — OSINT 的其余部分没有它也能工作。

3 — ABUSEIPDB

它回答什么：这个地址是否被举报过滥用 — 垃圾邮件、攻击、扫描 — 人群对此有多大把握？OSINT 会把它显示为一个满分 100 的滥用置信度评分，并附有报告数量。在四个密钥中，这是应用自己称为最好的 “这个地址是否被举报过行为不端？” 评分的那个。

去哪里：abuseipdb.com

1. 选择 Register («注册») 并选择 Individual FREE («个人免费») 套餐。免费就是免费 — 永远不需要卡。
2. 填写你的名、姓、电子邮件地址和国家，以 Individual («个人») 身份注册。用户名框可以留空。
3. 设置你的密码并通过 “I'm not a robot” («我不是机器人») 检查。网站会回答：“Your account has been created” («你的账户已创建»)。
4. 在做任何其他事情之前先验证你的电子邮件。打开它们发送的验证电子邮件并点击其中的链接。在你做这一步之前，Keys («密钥») 页面会一直被锁定 — 这是每个人都会漏掉的一步。
5. 回到网站上，打开你的 Account («账户»), 然后是 API Keys («API 密钥»)。创建一个密钥 (名称由你决定 — “My App” («我的应用») 就很好)。
6. 按下 Show («显示») 显示密钥，并复制完整的密钥。§ 6 会告诉你它在 OSINT 中应该放在哪里。

免费层级：Individual 套餐永远免费 — 1,000 次检查和报告 — 注册页面在你注册之前就用通俗的话说明了这一点。

之后没有需要按的按钮：一旦你的 AbuseIPDB 密钥保存在 OSINT 中 (§ 6)，应用就会自己为你面板上的外部地址运行这项检查。它的答案会出现在详情窗格的 WHAT THE CHECKS SAID («检查说了什么») 下面，在 AbuseIPDB 那一行 — 评分、报告数量，以及它上次发言的时间。

4 — GREYNOISE

它回答什么：这个地址是互联网背景噪声的一部分 — 冲刷着每一个人的无尽扫描 — 还是更罕见的东西？GreyNoise
还保存着一组已知良性服务，所以一个著名、行为良好的地址会被准确地读作那样。

去哪里：greynoise.io

1. 选择 Sign Up («注册») 并选择免费的 Personal («个人») 电子邮件选项。
2. 输入你的电子邮件地址并设置一个密码。
3. 完成你的个人资料 — 名和姓（称谓框可以留空）。在保存这些之前，网站不会打开其余部分。
4. 点击它们通过电子邮件发给你的验证链接。你的免费账户现在已经激活。

现在是诚实的部分 — 在去寻找密钥之前先读完这一段：个人电子邮件账户不包含 API 密钥。GreyNoise 在账户自己的页面上这样说明：密钥是提供给工作电子邮件账户的。这是它们的规则，没有某个你错过的隐藏的免费密钥页面。

好消息是：OSINT 不需要密钥。Check with GreyNoise («用 GreyNoise 检查») 按钮在完全没有密钥的情况下也能工作，在一个小的每日免费额度内。当当天的额度用完时，窗格会用通俗的话说明 — “Free allowance used up — press the button again tomorrow” («免费额度已用完 — 请明天再按这个按钮») — 并且其他每一项检查都会继续工作。

如果你确实有工作电子邮件（你自己公司或组织的地址 — 不是 Gmail）：你可以用它创建一个 GreyNoise 账户，那个账户确实带有一个密钥，显示在其账户设置中。像其他密钥一样把它粘贴到 OSINT 中 (§ 6)。它能买到的只是多一点额度 — 应用自己说得很明白：一个密钥会 “raises the tiny free GreyNoise allowance a little” («把微小的 GreyNoise 免费额度稍微提高一点») (免费密钥大约每周 50 次查询)。没有人需要它；它在那里，以备你哪天想要。

5 — ABUSE.CH (URLHAUS 密钥)

它回答什么：abuse.ch 运营着 URLhaus，一份被抓到提供恶意软件链接的主机名单。OSINT 会问：这个主机是否提供过恶意软件链接？这里的一个“是”是响亮的答案 — 窗格会显示一行点名该威胁的警告。

去哪里：auth.abuse.ch — abuse.ch 的登录之家。

1. 在 sign-in link by email («通过电子邮件发送登录链接») 框中输入你的电子邮件地址。
2. 通过 “Verify you are human” («验证你是真人») 检查 — 真人一秒就能通过；它在那里是为了把机器人挡在一个免费服务之外。
3. 按下 “Email me a sign-in link” («通过电子邮件给我发送登录链接»)。
4. 打开到达的电子邮件并点击其中的登录链接。不需要发明的密码 — 链接就是这扇门的钥匙。
5. 你的个人资料页面会显示你的 Auth-Key。复制完整的密钥。§ 6 会告诉你它在 OSINT 中应该放在哪里 — 放进标有 abuse.ch Auth-Key 的字段中。

免费层级：abuse.ch 账户是免费的。你个人资料上的 Auth-Key 是 OSINT 需要从它们那里得到的唯一凭据。

6 — 把你的密钥放入 OSINT

每一个密钥走的都是同一条路。每个服务做一次，按任何顺序，在你拿到每个密钥时做 — OSINT 不需要全部四个，并且每一个都会在保存的那一刻开启。

1. 打开 OSINT。
2. 按下 Settings («设置») 按钮 (底部栏)。OSINT — Settings («OSINT — 设置») 窗口会打开。
3. 找到你的服务对应的字段。窗口会按这个顺序显示四个：AbuseIPDB key («AbuseIPDB 密钥»)、VirusTotal key («VirusTotal 密钥»)、abuse.ch Auth-Key («abuse.ch 身份验证密钥»)、GreyNoise key («GreyNoise 密钥»)。
- 每个字段都会把你输入的内容藏在圆点后面，并且在每个字段下方，应用都会提醒你：“Key saved on this computer only” («密钥仅保存在这台电脑上»)。
4. 把完整的密钥粘贴到它的字段中 — 开头和结尾不要有空格。
5. 按下 Save Settings («保存设置»)。
- 窗口会回答：“Saved — on this computer only” («已保存 — 仅在这台电脑上»)。
- 这就完成了 — 密钥在重新启动后仍会保存；你不用再粘贴一次。

字段名称，与 § 2–§ 5 对应：VirusTotal 密钥 (§ 2) → VirusTotal key 字段 AbuseIPDB 密钥 (§ 3) → AbuseIPDB key 字段 GreyNoise 密钥 (§ 4，仅限工作电子邮件账户) → GreyNoise key 字段 abuse.ch Auth-Key (§ 5) → abuse.ch Auth-Key 字段 — 这就是开启 URLhaus 检查的密钥

产品的实情，通俗地说

- **保存就是保存。** Save Settings 会写入窗口中的每一个字段 — 永久保存，直到你更改它。
- **一个文件、你的电脑、你的账户。** 这些密钥只保存在 OSINT 的本地设置文件中，并已锁定为只有你自己的用户账户可以读取 (文件权限 0600)。该文件从不上传到任何地方，也从不属于任何下载的一部分。
- **密钥是秘密。** 像对待房门钥匙一样对待它：不要发布它，不要到处通过消息发送它，不要把它粘贴到莫名其妙要求它的网页中。它唯一会去的地方是签发它的服务和 OSINT 的 Settings 字段。
- **移除一个密钥：** 打开 Settings，清空该字段，按下 Save Settings。该检查会重新关闭 (对于 GreyNoise，按钮只是回到它的免费无密钥额度)。
- **更换一个密钥：** 把新密钥粘贴覆盖旧密钥并 Save («保存»)。完成。

7 — 运行检查

1. 在面板上，点击一条连接。面板下方的详情窗格会显示那条连接 — 它是谁，以及检查对它说了什么。
2. 窗格下方是检查按钮：Copy IP («复制 IP»)、Check with GreyNoise («用 GreyNoise 检查»)、Check with VirusTotal («用 VirusTotal 检查»)、Check with URLhaus («用 URLhaus 检查»)。
- 按下你想要的那个。
3. 窗格会告诉你检查正在运行，它的答案会落在同一个窗格中，位于 WHAT THE CHECKS SAID («检查说了什么») 下面。

这些按钮只作用于你选择的那条连接，并且只在你按下它们时才作用 — 并且它们作用于外部 (公共) 连接。选择你自己家庭网络内的一行，窗格会告诉你：“Pick an outside connection first” («请先选择一条外部连接»)。

关于你自己的私有地址，永远不会发送任何东西出去。

每个答案的含义，一行说清

- **VirusTotal:** “N engines say malicious · N suspicious · N harmless” (N 个引擎说恶意 · N 个可疑 · N 个无害) — 扫描器的投票，公开计数。
- **AbuseIPDB:** “Abuse confidence N/100 · N reports” (滥用置信度 N/100 · N 份报告) — 举报人群有多强烈地认为这个地址行为不端。没有按钮：保存密钥后，这项检查会自己运行，它的那一行会与其他行一起出现。
- **GreyNoise:** 该地址是否 “seen scanning the internet” (被看到正在扫描互联网)、它被归为哪一类，以及它是否位于已知良性服务集合中 — 背景噪声，还是带有你名字的东西。
- **URLhaus:** 没有内容可说时保持安静；一条 ⚠ 警告行 — “This host has served malware links” (这个主机提供过恶意软件链接) — 当有内容时出现。

在那些行上方，窗格会给出判定 — 对检查所说一切的最坏的诚实解读：KNOWN

BAD、SUSPICIOUS、KNOWN SAFE，或者 NO BAD

REPORTS (应用会小心地说明这不是一个保证它安全的承诺) — 后面跟着一个用通俗的话写的 WHAT SHOULD I DO? (我该怎么做?) 部分。

还没有密钥？这些按钮会说实话，而不是悄悄失败。在没有保存密钥的情况下按下 Check with VirusTotal，窗格会回答：“VirusTotal is OFF — add your own free key in Settings to turn it on” (VirusTotal 已关闭 — 在 Settings 中添加你自己的免费密钥以开启它)。URLhaus 会以同样的方式回答：“URLhaus needs your free abuse.ch key — add it in Settings” (URLhaus 需要你的免费 abuse.ch 密钥 — 在 Settings 中添加它)。GreyNoise 什么都不要求 — 它直接运行。

8 — 密钥安全 + 当有东西看起来不对时

- **密钥泄露了？** 回到那个服务，创建一个新密钥并删除旧密钥 — 本指南中的每一个服务都让你能做这两件事 — 然后把新密钥粘贴到 OSINT 中 (§ 6)。旧密钥会在服务那里失效，所以一份泄露的副本毫无用处。
- **“Free allowance used up” (免费额度已用完) (GreyNoise) :** 这不是错误。免费当天的检查已经用完；按钮明天会再次工作，今晚其他一切都会继续工作。
- **一项检查说 “failed” (失败) :** 该服务没有回答 — 窗格会把该地址显示为对该检查未知，从不显示为已通过。稍后再试；一个诚实的 “没有答案” 是设计，不是错误。
- **在任何地方被要求提供卡：停下来。** 本指南中的每一个密钥都是免费的。要求提供卡意味着误选了一个付费套餐 — 退出并选择步骤中提到的免费套餐。
- **弄丢了你创建的密钥？** 重新登录该服务 — VirusTotal 和 abuse.ch 会在你的个人资料/API 页面上显示你的密钥；在 AbuseIPDB 上，按下你创建的密钥旁边的 Show (显示)。然后再走一遍 § 6。

这就是全部了。四个免费密钥，每一个都从它自己的服务获取，粘贴一次到 Settings 中，从你自己的电脑上工作 — 以及一个会清楚告诉你它发送了什么、找到了什么、不知道什么的应用。检查你的机器在和谁通信。这就是 OSINT 的用途。

OSINT — Live Connections Viewer • 777 Software。本指南随应用一起提供。这里提到的服务由它们自己的人员运营；它们的注册页面可能会随时间重新安排摆设，但其形态 — 免费账户、验证你的电子邮件、在你的个人资料上找到密钥 — 不会改变。