Dr.WEB

Enterprise Security Suite

安装手册



© Doctor Web, 2021. 版权所有

本手册是关于手册所涉及的Dr.Web家族软件产品的信息性介绍和帮助手册。本手册不可成为全面判断Dr.Web家族软件产品具备或不具备某些功能和/或技术参数的依据，亦不可用于判定Dr.Web家族软件产品是否符合某些要求、技术任务和/或参数以及其他第三方文件。

本手册中的所有资料为Doctor Web公司所有并只能为产品购买者个人使用。本手册的任何部分均不得复制、转载于网络资源或利用通讯渠道或在大众媒体加以传播，不得以个人使用以外的任何其他方式不指明出处加以利用。

商标

Dr.Web、SpIDer Mail、SpIDer Guard、CureIt!、CureNet!、AV-Desk、KATANA和徽标Dr.WEB是Doctor Web公司在俄罗斯以及/或者其他国家的注册商标。本文档中提及的其他注册商标、徽标和公司名称为其所有人所有。

免责声明

任何情况下Doctor Web公司及其经销商对本文档可能的任何错误和/或遗漏以及因其导致的产品购买方损失（直接或间接损失，包括未得利益）均不承担任何责任。

Dr.Web Enterprise Security Suite
版本 12.0
安装手册
2021/2/20

Doctor Web有限公司 俄罗斯总公司

地址：125124，亚姆斯基场3道街2-12A

网址：https://www.drweb.com/

电话：+7(495)789-45-87

公司在其他地区和国家分支机构的相关信息见公司官网。

Doctor Web

Doctor Web公司是俄罗斯信息安全产品厂商。

Doctor Web公司为国家机关和大型企业以及个人用户提供高效反病毒和反垃圾邮件解决方案。

Dr.Web家族反病毒解决方案的研发始于1992年，一直以来展示着卓越的恶意软件侦测能力，符合国际安全标准。

各种证书与奖项以及用户遍布全球是对我公司产品无比信任的见证。

感谢用户对Dr.Web家族反病毒解决方案的支持！

内容

第一章、导言 6
1.1. 文档用途 6
1.2. 标志与缩写 7
第二章、Dr.Web Enterprise Security Suite 9
2.1. 关于产品 9
2.2. 系统要求 16
2.3. 供货方案 20
第三章、授权 22
第四章、开始运行 23
4.1. 反病毒网络的部署 23
4.2. 网络连接设置 25
4.2.1. 直接连接 26
4.2.2. Dr.Web服务器搜索服务 27
4.2.3. 使用SRV协议 27
4.3. 保障安全连接 28
4.3.1. 流量加密和压缩 28
4.3.2. 安全连接保障工具 32
4.3.3. 将客户端连接到Dr.Web服务器 34
4.4. Dr.Web Enterprise Security Suite与Active Directory的集成 35
第五章、安装Dr.Web Enterprise Security Suite组件 37
5.1. 安装Dr.Web服务器 37
5.1.1. OS Windows下Dr.Web服务器的安装 37
5.1.2. UNIX家族操作系统Dr.Web服务器的安装 42
5.2. 安装Dr.Web代理端 43
5.2.1. 安装文件 44
5.2.2. 本地安装Dr.Web代理端 46
5.2.3. OS Windows下Dr.Web代理端的远程安装 53
5.3. NAP Validator的安装 63
5.4. Dr.Web代理服务器的安装 64
5.4.1. 创建Dr.Web代理服务器账户 64
5.4.2. 在安装Windows操作系统Dr.Web代理端的过程中安装Dr.Web代理服务器 66
5.4.3. 利用安装程序安装Dr.Web代理服务器 66
5.4.4. Dr.Web代理服务器连接Dr.Web服务器 69

第六章、删除Dr.Web Enterprise Security Suite组件 71
6.1. 卸载Dr.Web服务器 71
6.1.1. OS Windows下Dr.Web服务器的卸载 71
6.1.2. UNIX家族操作系统Dr.Web服务器的卸载 71
6.2. 删除Dr.Web代理端 72
6.2.1. 删除OS Windows下的Dr.Web代理端 72
6.2.2. 通过Active Directory服务删除代理端 74
6.3. 删除Dr.Web代理服务器 74
6.3.1. 本地删除Dr.Web代理服务器 75
6.3.2. 远程删除Dr.Web代理服务器 75
第七章、更新Dr.Web Enterprise Security Suite组件 77
7.1. OS Windows下Dr.Web服务器的更新 77
7.2. UNIX家族操作系统Dr.Web服务器的更新 82
7.3. 更新Dr.Web代理端 88
7.3.1. OS Windows工作站Dr.Web代理端的更新 88
7.3.2. OS Android工作站Dr.Web代理端的更新 89
7.3.3. OS Linux和macOS工作站Dr.Web代理端的更新 90
7.4. 更新Dr.Web代理服务器 90
7.4.1. 在运行过程中更新Dr.Web代理服务器 90
7.4.2. 通过安装程序更新Dr.Web代理服务器 91
索引 93

第一章、导言

1.1. 文档用途

Dr.Web Enterprise Security Suite反病毒网络管理员手册包含利用 Dr.Web Enterprise Security Suite建立企业计算机网络全面反病毒保护网络的总体原则以及具体实施细则。

反病毒网络管理员手册由以下几部分组成：

1. **安装手册(drweb-12.0-esuite-install-manual-cn.pdf)**

   将有助于企业领导作出购买、安装反病毒全面保护系统的决定。

   安装手册介绍反病毒网络部署流程和基本组件安装流程。

2. **管理员手册(drweb-12.0-esuite-admin-manual-cn.pdf)**

   供*反病毒网络管理员*使用，该管理员的职责是对企业网络中计算机(工作站和服务器)的反病毒保护进行管理。

   反病毒网络管理员应具备系统管理员的职能或者与内网管理员协作，应掌握反病毒保护策略并熟知适用于内网中各操作系统的Dr.Web反病毒软件包。

3. **附录(drweb-12.0-esuite-appendices-cn.pdf)**

   包含技术信息，介绍设置反病毒软件组件使用的参数以及运用参数的规则和各规则的含义。



上述各文档间存在交叉索引。将文档加载到本地计算机时，只有当所有文件处于同一目录且保留原有名称的情况下，交叉索引才可正常使用。

随附手册还包括：

1. **反病毒网络部署说明**

   内容为反病毒网络组件安装和初步设置的简短介绍。详细信息请查阅管理员手册。

2. **工作站管理手册**

   介绍反病毒管理员如何通过Dr.Web安全管理中心统一设置工作站上安装的反病毒软件。

3. **用户手册**

   介绍可直接在受保护工作站上进行的Dr.Web反病毒解决方案的设置。

4. **Web API手册**

   为利用Web API将Dr.Web Enterprise Security Suite与第三方软件集成的技术信息。

5. **Dr.Web服务器数据库手册**

   为Dr.Web服务器数据库内在结构和使用说明。

所有上述手册作为Dr.Web Enterprise Security Suite组成，可通过Dr.Web安全管理中心打开。

在阅读手册前请确认您使用的产品当前版本的相应手册的最新版本。手册内容不断更新，您可在Doctor Web公司官方网站获取手册的最新版本https://download.drweb.com/doc/。

1.2. 标志与缩写

标志说明

本手册中使用以下标志：

标志	说明
	重要说明或指令
	可能出现错误的情况或需要特别注意的重要环节。
反病毒网络	新的专有名词或描述中所含专有名词。
<IP-address>	用实际值代替名称的占位符
保存	按钮、窗口、菜单选项或其他程序界面元素的名称
CTRL	键盘按键名称
`C:\Windows\`	文件和文件夹以及部分程序代码的名称
附录 A	手册章节的交叉链接或外部资源的超链接

缩写

本手册中可能出现以下缩写：

- ACL——访问控制列表(Access Control List)，
- CDN——内容分发网络(Content Delivery Network)，
- DFS——分布式文件系统(Distributed File System)，
- DNS——域名系统(Domain Name System)，
- FQDN——全限定域名(Fully Qualified Domain Name)，
- GUI——图形用户界面(Graphical User Interface)，GUI-程序版本——使用GUI的版本，
- MIB——管理信息库(Management Information Base)，
- MTU——最大传输单元(Maximum Transmission Unit)，
- NAP——Network Access Protection，
- TTL——数据包生存时间(Time To Live)，
- UDS——UNIX域套接字(UNIX Domain Socket)，
- DB、DBMS——数据库、数据库管理系统，
- GUS Dr.Web——全球更新系统 Dr.Web，
- LAN——局域网，
- OS——操作系统，

- Software——软件。

第二章、Dr.Web Enterprise Security Suite

2.1. 关于产品

Dr.Web Enterprise Security Suite用于组织和管理可靠的统一保护系统，为包括移动设备和员工家用电脑在内的公司局域网提供全面的反病毒保护。

安装有能够交互作用的Dr.Web Enterprise Security Suite组件的所有计算机和移动设备构成统一的*反病毒网络*。



图**1-1.反病毒网络逻辑结构**

Dr.Web Enterprise Security Suite反病毒网络为*服务器-客户端*结构。其组件安装到用户和管理员的电脑和移动设备，以及在局域网执行服务器功能的计算机。反病毒网络组件使用TCP/IP协议相互交换信息。既可通过局域网，也可通过互联网将反病毒软件包安装到受保护工作站（并在安装后对其进行管理）。

统一保护服务器

统一保护服务器安装于反病毒网络中的任何一台电脑，而且不一定要安装的在局域网执行服务器功能的计算机。对电脑的基本系统要求参见系统要求。

服务器软件为多平台软件，可使用以下操作系统的计算机作为服务器：

- OS Windows，
- UNIX家族操作系统（Linux、FreeBSD）。

统一保护服务器保存用于受保护计算机各种操作系统的反病毒软件包、病毒库、反病毒软件包的更新以及用户密钥和受保护计算机软件包设置。服务器通过互联网从全球更新系统服务器获取反病毒组件和病毒库更新并将更新分发至受保护工作站。

可使用由多个服务器组成的集群管理反病毒网络中的受保护工作站。

服务器支持重要数据（数据库、配置文件等）备份功能。

服务器记录统一的反病毒网络事件日志。

统一数据库

统一数据库连接统一保护服务器，保存反病毒网络事件统计数据、服务器本身的设置、受保护工作站参数和安装于受保护工作站的反病毒组件的参数。

可使用以下类型的数据库：

内设数据库。是统一管理服务器内置的数据库SQLite3。

外设数据库。内置驱动程序可理解以下数据库：

- MySQL，
- Oracle，
- PostgreSQL（包括Postgres Pro）、
- ODBC驱动程序：用于连接其它数据库，如Microsoft SQL Server/Microsoft SQL Server Express.

可使用任意一种能够满足需要的数据库。选择时应遵循对数据库的要求，如：可用于相应规模的反病毒网络；数据库软件使用特点；数据库本身的管理功能以及企业具体要求和标准。

统一保护管理中心

统一保护管理中心和服务器一起自动安装，是Web界面，通过编辑服务器设置以及保存于服务器和受保护计算机上的受保护计算机设置来对服务器和反病毒网络进行管理。

管理中心可在任何一台能够与服务器. 建立网络连接的计算机上打开。几乎所有操作系统下都可使用管理中心，可支持其所有功能的浏览器为：

- Windows Internet Explorer，
- Microsoft Edge，
- Mozilla Firefox，
- Google Chrome。

可能方案参见系统要求。

统一保护管理中心具有以下功能：

- 便于将反病毒软件安装到受保护工作站，包括：预先在网络中搜索计算机后对OS Windows工作站进行远程安装；创建带有独有识别码和服务器连接参数的软件版本，以简化管理员进行

反病毒软件的安装或让用户能够将反病毒软件自行安装到工作站（详见安装Dr.Web代理端）。

- 利用组机制简化对反病毒网络工作站的管理。
- 对工作站上的反病毒软件包进行统一管理，包括删除OS Windows 工作站上的部分组件或整个反病毒软件；设置反病毒软件包组件运行参数；为工作站用户指定设置和管理受保护工作站的权限。
- 对工作站反病毒扫描进行统一管理，包括：按照日程或管理员从管理中心发出的指令远程启动反病毒扫描；统一设置反病毒扫描参数，这些参数会发送到工作站并以指定参数启动本地扫描。
- 获取受保护工作站状态统计信息、病毒统计信息、已安装的反病毒软件包状态、已启用的反病毒组件状态以及受保护工作站硬软件配置列表。
- 具备灵活的服务器和反病毒网络管理系统，可限定不同管理员的权限，且管理员可通过外部身份验证系统Active Directory、LDAP、RADIUS和PAM 登录。
- 管理工作站反病毒保护授权，可利用分支系统为工作站、工作站组指定授权，还可在多服务器反病毒网络中的不同服务器间传递授权。
- 利用设置选项可为服务器和其组件灵活指定配置，包括：为服务器指定维护日程；接入用户进程；灵活设置更新系统，从GUS获取反病毒网络所有组件的更新并将其传播到工作站；设置管理员反病毒网络事件通知系统，可选择不同方式送达通知；设置服务器间连接，管理多服务器反病毒网络的配置。



功能使用详细信息参见**管理员手册**。

Dr.Web安全管理中心的一个组成部分是与服务器一同自动安装的Web服务器。Web服务器的主要任务是保证运行管理中心页面和客户端网络连接。

统一保护移动管理中心

另一单独组件是移动管理中心，在iOS和Android设备安装运行。对应用程序的基本要求参见系统要求。

移动管理中心连接服务器使用的是反病毒网络管理员账户，包括使用加密协议进行连接。移动管理中心 具备 管理中心的基本功能：

1. 管理Dr.Web服务器库：
   - 查看库中产品状态；
   - 启动从Dr.Web全球更新系统进行库更新。
2. 管理反病毒软件包更新出错的工作站：
   - 显示出错的工作站；
   - 在出错的工作站更新组件。
3. 收集反病毒网络状态信息：
   - 在Dr.Web服务器注册的工作站数量，其当前状态（在线/离线）；
   - 受保护工作站感染统计信息。
4. 管理等待与Dr.Web服务器连接的新工作站：
   - 批准访问；
   - 拒绝工作站。

5. 管理反病毒网络工作站上安装的反病毒组件：
   - 在所选工作站或所选组的所有工作站启动快速扫描或完全扫描；
   - 设置Dr.Web扫描仪侦测到恶意对象时的反应；
   - 查看和管理所选工作站或所选组的所有工作站上隔离区文件。
6. 管理工作站和工作站组：
   - 查看设置；
   - 查看和管理反病毒软件包组件；
   - 删除；
   - 向工作站发送自定义内容的通知；
   - 重启OS Windows工作站；
   - 添加至快速访问收藏项。
7. 按照不同参数在反病毒网络查找工作站和工作站组：按名称、地址和ID。
8. 通过Push及时对话系统查看并管理反病毒网络重要事件通知：
   - 在Dr.Web服务器显示所有通知；
   - 指定对通知事件的反应；
   - 按照指定的过滤参数搜索通知；
   - 删除通知；
   - 禁用自动删除通知。

可从管理中心下载移动管理中心或直接在App Store和Google Play下载。

保护网络中的工作站

在网络中的受保护工作站和移动设备安装管理模块（客户端）和用于相应操作系统的反病毒软件包。

软件支持多种平台软件，可对以下操作系统的计算机和移动设备进行反病毒保护：

- OS Windows，
- UNIX家族操作系统，
- macOS，
- OS Android。

受保护工作站可以是用户电脑，也可以是局域网中的服务器，包括对Microsoft Outlook邮件系统实施反病毒保护。

管理模块定期从服务器获取反病毒组件和病毒库更新，并向服务器发送受保护计算机上的病毒事件信息。

如统一保护服务器无法访问，可直接通过互联网从全球更新系统更新受保护工作站上的病毒库。

分别为不同操作系统的工作站提供的保护功能见下。

OS Windows工作站

反病毒扫描

按照用户调用或日程对计算机进行扫描。还可从管理中心远程启动工作站扫描，包括检查是否存在Rootkit。

文件监视器

实时模式下对文件系统进行不间断检查，检查所有启动的进程，以及在硬盘创建的文件和在移动设备打开的文件。

邮件监视器

使用邮件客户端时检查所有进出邮件。

还可进行垃圾邮件过滤（如授权允许使用这一功能）。

Web 监视器

检查所有使用http协议对网站的访问。消除http流量存在的威胁（如获取和发送的文件中存在的威胁），阻止访问可疑的资源和错误资源。

办公控制

控制对本地资源和网络资源的访问，包括控制对网站的访问。可监控重要文件的完整性，防止无意更改或病毒感染，禁止员工访问不需要的信息。

防火墙

保护计算机免于未经授权的外部访问，防止重要信息通过互联网泄露。控制互联网连接和数据传输，在数据包和应用程序层面阻止可疑的连接。

隔离区

将恶意对象和可疑对象隔离到专门的文件夹。

自我保护

保护Dr.Web Enterprise Security Suite文件和目录，防止未经授权进行删除、被用户无意间删除修改或被恶意软件修改。启用自我保护时只允许Dr.Web进程访问Dr.Web Enterprise Security Suite的文件和目录。

预防性保护

预防潜在危险。监控对操作系统重要对象的访问，监控驱动程序的加载以及自启动软件和系统服务的运行，并跟踪已启动进程，如发现病毒活动则阻断进程。

应用程序监控

对工作站所有进程的活动进行监控，可让反病毒网络管理员调整受保护工作站上的应用是否允许使用或禁止使用。

UNIX家族操作系统工作站

反病毒扫描

扫描引擎。执行数据（文件内容、磁盘设备启动记录、来自Dr.Web for UNIX其他组件的数据）的反病毒扫描。安排扫描次序。对可清除的威胁进行清除。

反病毒扫描、管理隔离区

文件系统对象扫描组件和隔离区管理器。接受来自Dr.Web for UNIX其他组件的文件扫描任务。按照日程巡视文件系统目录，将文件提交给扫描引擎进行扫描。删除已感染文件，隔离文件或从隔离区还原文件、管理隔离区目录。保证缓存保存的是已检查文件和已侦测到的威胁注册表的最新信息。

供所有检查文件需对象的组件使用，如SpIDer Guard（for Linux、SMB、NSS）。

扫描Web流量

ICAP服务器，对申请和经代理服务器的HTTP流量进行分析。阻断已感染文件的传输，阻止访问不良Web资源和系统管理员列入黑名单的网络节点。

用于GNU/Linux系统的文件监视器

Linux文件系统监视器。以背景模式运行，监控GNU/Linux文件系统中执行的文件操作（如创建文件，打开、关闭和启动文件）。向文件扫描组件申请对新创建文件和内容更改的文件以及软件启动时的执行文件进行扫描。

用于Samba目录的文件监视器

Samba共享文件监视器。以背景模式运行，监控文件系统中对划分给SMB服务器文件库Samba的目录的操作（如创建文，打开、关闭文件，只读和写入操作）。向文件扫描组件申请对新创建文件和内容更改的文件进行扫描。

NSS文件监视器

NSS卷（Novell Storage Services）监视器。以背景模式运行，监控文件系统指定节点的NSS卷中的操作（如创建文件，打开、关闭文件以及写入操作）。将新创建文件和内容更改的文件发送给文件扫描组件进行扫描。

检查网络连接

对网络流量和URL进行检查的组件。负责检查从网络加载到本地节点和从本地节点上传到外网的数据是否存在威胁，阻止访问不良Web资源和系统管理员列入黑名单的网络节点。

邮件监视器

对邮件进行检查的组件。分析邮件协议通知、解析电子邮件以备检查是否含有威胁。有两种运行模式：

1. 邮件服务器（Sendmail, Postfix等等）过滤器，利用Milter、Spamd或Rspamd接口接入。
2. 透明代理邮件协议（SMTP, POP3, IMAP）。这种模式下使用SpIDer Gate。

macOS工作站

反病毒扫描

按照用户调用或日程对计算机进行扫描。还可从管理中心远程启动工作站扫描。

文件监视器

实时模式下对文件系统进行不间断检查，检查所有启动的进程，以及在硬盘创建的文件和在移动设备打开的文件。

Web 监视器

检查所有使用http协议对网站的访问。消除http流量存在的威胁（如获取和发送的文件中存在的威胁），阻止访问可疑的资源和错误资源。

隔离区

将恶意对象和可疑对象隔离到专门的文件夹。

OS Android 移动设备

反病毒扫描

按照用户调用或日程对移动设备进行扫描。还可从管理中心远程启动工作站扫描。

文件监视器

实时模式下对文件系统进行不间断检查。在试图将文件保存到移动设备时对其进行检查。

来电和短信过滤

过滤SMS短信和电话可阻止不需要接听的电话和接收的短信，如广告短信和来自未知号码的电话和短信。

防盗器

在移动设备丢失或被窃时确定其所在地或及时上锁。

限制访问互联网资源

URL过滤器使移动设备用户远离不良网路资源。

防火墙

保护移动设备免于未经授权的外部访问，防止重要信息通过互联网泄露。控制互联网连接和数据传输，在数据包和应用程序层面阻止可疑的连接。

帮助解决安全问题

对移动设备安全状态进行诊断和发现，消除发现的问题和漏洞。

控制应用程序的启动

禁止在移动设备启动管理员允许启动列表中不包含的应用程序。

保证反病毒网络各组件间的连接

可利用以下功能保证反病毒网络各组件间的连接稳定、安全：

Dr.Web代理服务器

代理服务器可选择性加入反病毒网络。代理服务器的主要任务——在无法建立直接连接的情况下保证服务器与受保护工作站的连接。

通过代理服务器可将反病毒网络中的任意一台计算机作为：

- 更新转发中心，这样可以降低服务器的网络负载和服务器与代理服务器的连接负载，利用缓存功能还可缩短受保护工作站获取更新的时间。
- 将受保护工作站病毒事件转发给服务器的转发中心，这样也可以降低网络负载，并在服务器和受保护工作站处于不同的网络的情况下保证数据的传输。

流量压缩

可使用专门算法压缩反病毒网络组件间传输数据，以便将网络流量降至最低。

流量加密

可反病毒网络组件间传输数据时进行加密，已提高保护等级。

补充功能

NAP Validator

NAP Validator是补充组件，用于使用Microsoft Network Access Protection（NAP）技术检查受保护工作站软件运行能力。通过执行对网络工作站运行能力的要求达到提高安全级别的目的。

库加载器

Dr.Web库加载器是补充工具，用于从全球更新系统加载Dr.Web Enterprise Security Suite 产品。可用于加载Dr.Web Enterprise Security Suite产品更新，并在获取更新后将其转至没有接通互联网的服务器。

2.2. 系统要求

Dr.Web Enterprise Security Suite的安装和正常运行要求：

- 反病毒网络计算机应能够访问Dr.Web服务器或Dr.Web代理服务器。
- 为保证反病毒组件间的互动，计算机上应打开以下端口：

端口号	协议	连接	用途
2193	TCP	• 服务器和代理服务器进出流量 • 代理端出港流量	用于连接反病毒组件与服务器和服务器间连接。 包括使用代理服务器与客户端建立连接。
	UDP	进港，出港	用于运行网络搜索仪。
139, 445	TCP	• 服务器出港流量 • 代理端进港流量	用于远程安装Dr.Web代理端
	UDP	进港，出港	
9080	HTTP	• 服务器进港流量 • 管理中心所在服务器出港流量	用于运行Dr.Web安全管理中心。
9081	HTTPS		
10101	TCP		用于运行服务器远程诊断工具。
80	HTTP	出港	用于从GUS获取更新。
443	HTTPS		

Dr.Web服务器

组件	系统要求
处理器	CPU支持SSE2，频率1.3 GHz或更高。

组件	系统要求
内存	• 最低要求：1GB。 • 建议使用：2GB以上。
硬盘空间	• 服务器软件需要至少50GB设置以及补充空间用于保存临时文件，如在Dr.Web服务器安装目录子目录 var\installers-cache保存代理端个人安装包（每个约17MB）。 • 数据库占用不高于5GB。 • 不论服务器安装于何处，OS Windows系统盘或UNIX家族操作系统的/var/tmp（如临时文件区有改动，则为另一临时文件区）： ▫ 服务器安装要求空间不小于4.3GB用于启动安装程序和解压临时文件； ▫ 服务器运行需要系统盘有可用空间用于保存临时文件和运行文件，这与数据库大小和库设置无关。
操作系统	• Windows(支持的操作系统完整列表见附录中的附录A)。 • Linux，需具备glibc 2.13或更高版本；包括ALT Linux 5.0或更高版本、Astra Linux Special Edition 1.3或更高版本。 • FreeBSD10.3或更高版本。
支持虚拟环境和云环境	支持在符合上述系统要求的操作系统于虚拟环境和云环境下运行，包括： • VMware； • Hyper-V； • Xen； • KVM。
其它	此外OS FreeBSD下还要求具备库compat-10x。 使用数据库Oracle要求具备库Linux kernel AIO access library (libaio)。

Dr.Web服务器不可安装到文件系统不支持符号链接的逻辑盘，比如FAT文件系统。

管理工具可在管理中心的**管理→工具**部分加载，应在满足Dr.Web服务器系统要求的计算机启动。

Dr.Web代理服务器

组件	系统要求
处理器	CPU支持SSE2，频率1.3 GHz或更高。
内存	不少于1GB。
硬盘空间	不少于1GB。

组件	系统要求
操作系统	• Windows(支持的操作系统完整列表见附录中的附录A)。 • Linux，需具备glibc 2.13或更高版本；包括ALT Linux 5.0或更高版本、Astra Linux Special Edition 1.3或更高版本。 • FreeBSD10.3或更高版本。

Dr.Web安全管理中心

a) 网络浏览器：

- Internet Explorer 11，
- Microsoft Edge 0.10或更高版本，
- Mozilla Firefox 44或更高版本，
- Google Chrome 49或更高版本，
- Opera最新版本，
- Safar最新版本。

使用网络浏览器Windows Internet Explorer时许注意：

- 在启用**Enhanced Security Configuration for Windows Internet Explorer**模式的网络浏览器Windows Internet Explorer不能保证管理中心完全正常运行。
- 如安装服务器的计算机名称中含有符号"_"（下划线），则不可在浏览器中利用管理中心操作服务器。这种情况下必须使用另一种网络浏览器。
- 正常运行管理中心需要在打开管理中心的浏览器的可信任网址中添加安装有Dr.Web服务器的计算机的IP地址和/或DNS名称。
- 在带有平铺界面的OS Windows 8和OS Windows Server 2012通过**开始**菜单正常打开管理中心需对网络浏览器进行以下设置：浏览**器属性→ 所有程序→ 打开Internet Explorer**勾选**总是以经典**视窗**在Internet Explorer**。
- 在浏览器Windows Internet Explorer使用加密协议https正常运行管理中心必须安装浏览器的所有最新更新。
- 浏览器Windows Internet Explorer使用兼容模式无法正常运行管理中心。

b) 运行管理中心建议使用的屏幕分辨率为1280x1024 px。

Dr.Web移动管理中心

安装应用的操作系统不同，系统要求也有所区别：

操作系统	系统要求	
	操作系统版本	设备
iOS	iOS 9及更高版本	Apple iPhone Apple iPad
Android	Android 4.1–10	–

NAP Validator

服务器端：

- OS Windows Server 2008。

代理端：

- OS Windows XP SP3、OS Windows Vista、OS Windows Server 2008。

Dr.Web代理端和反病毒软件包

系统要求取决于反病毒解决方案安装于何种操作系统（支持的操作系统完整列表见**附**录中的附录A. 支持的操作系统版本完整列表）：

- OS Windows：

组件	系统要求
处理器	CPU频率1GHz或更高。
可用内存	不少于512MB。
硬盘可用空间	不少于1GB用于执行文件以及用于运行日志和临时文件的补充空间。
其它	1. 正常显示**Windows操作系统Dr.Web代理端**帮助需使用Windows Internet Explorer 6.0或更高版本。 2. 插件Dr.Web for Outlook要求具备从Microsoft Office安装的Microsoft Outlook客户端： • Outlook 2000； • Outlook 2002； • Outlook 2003； • Outlook 2007； • Outlook 2010 SP2； • Outlook 2013； • Outlook 2016； • Outlook 2019。

- Linux家族操作系统：

组件	系统要求
处理器	处理器架构和指令系统 • Intel/AMD：为32位（IA-32, x86）、64位（x86-64, x64, amd64）； • ARM64。
可用内存	不少于512MB（推荐为1GB或更多）。
硬盘可用空间	反病毒软件目录所在卷可用磁盘空间不少于500MB。

- macOS、OS Android：配置要求与操作系统要求相符。

支持Dr.Web代理端在符合上述系统要求的操作系统于虚拟环境和云环境下运行，包括：

- VMware；
- Hyper-V；
- Xen；
- KVM。



在Dr.Web Enterprise Security Suite管理的反病毒网络工作站不应使用其他反病毒软件（包括其他版本的Dr.Web反病毒软件产品）。

2.3. 供货方案

软件**Dr.Web Enterprise Security Suite**根据所选**Dr.Web**服务器操作系统供货：

1. UNIX家族操作系统：
   - `drweb-<数据包版本>-<编号>-esuite-server-<操作系统版本>.tar.gz.run`
     Dr.Web服务器软件*
   - `drweb-reploader-<操作系统>-<位数>`
     Dr.Web库加载器控制台版本。
2. OS Windows：
   - `drweb-<数据包版本>-<编号>-esuite-server-<操作系统版本>.exe`
     Dr.Web服务器软件*
   - `drweb-<数据包版本>-<编号>-esuite-agent-full-windows.exe`
     Dr.Web代理端完整安装程序。
   - `drweb-reploader-windows-<位数>.exe`
     Dr.Web库加载器控制台版本。
   - `drweb-reploader-gui-windows-<位数>.exe`
     Dr.Web库加载器图形版本。

***Dr.Web**服务器软件包含以下组件：

- 支持相应操作系统的Dr.Web服务器软件，
- Dr.Web服务器安全数据，
- Dr.Web安全管理中心软件，
- 用于所支持的操作系统的Dr.Web代理端软件和反病毒软件包，
- 用于Windows操作系统的Dr.Web代理端更新模块，
- 用于Windows操作系统的Dr.Web反垃圾邮件，
- 用于Windows操作系统的Dr.Web病毒库、反病毒专家内置过滤器数据库和反垃圾邮件数据库，
- 帮助文档，

- Doctor Web公司新闻。

除软件外还提供序列号，注册序列号后您会获得授权密钥文件。

安装Dr.Web服务器后可从全球更新系统将以下Dr.Web企业产品加载到库中：

- 用于Windows操作系统的Dr.Web代理端完整安装程序，
- 安装到OS UNIX（包括局域网服务器）、Android、macOS受保护工作站的产品，
- Dr.Web for IBM Lotus Domino，
- Dr.Web for Microsoft Exchange Server，
- Dr.Web代理服务器，
- 用于Active Directory的Dr.Web代理端，
- Active Directory架构更改工具，
- Active Directory对象参数更改工具，
- NAP Validator。



使用服务器库的详细信息参见**管理员手册**中的Dr.Web服务器库的管理。

第三章、授权

使用反病毒解决方案Dr.Web Enterprise Security Suite需要具备授权。

Dr.Web Enterprise Security Suite反病毒解决方案使用授权的组成和价格取决于受保护工作站的数量，包括在Dr.Web Enterprise Security Suite网络中作为受保护工作站的服务器数量。

在购买Dr.Web Enterprise Security Suite解决方案时一定要告知授权销售商这一信息。所使用的Dr.Web 服务器数量不影响授权价格。

授权密钥文件

Dr.Web Enterprise Security Suite使用权通过授权密钥文件来控制。

授权密钥文件格式使用电子签名防止文件被修改。编辑文件会使密钥文件失效。为防止密钥文件意外受损，请不要对其进行修改和/或在文件编辑器查看文件后进行保存。

授权密钥文件以zip压缩文档形式提供，包含一个或几个用于受保护工作站的密钥文件。

用户可利用以下一种方式获取授权密钥文件：

- 授权密钥文件有可能包含于购买的Dr.Web Enterprise Security Suite反病毒软件中，如果制作软件包时纳入了授权密钥文件。但一般产品随附的只是序列号。
- 用户在Doctor Web公司地址为https://products.drweb.com/register/v4/网页（如产品所附注册卡中未标明其它地址）注册序列号后，授权密钥文件通过电子邮箱发送给用户。请登录指定网页，填写客户信息表并输入序列号（序列号印于注册卡）。密钥文件压缩文档会发送至您所指定是邮箱。也可从此网站直接加载密钥文件。
- 授权密钥文件可通过单独载体提供。

建议在授权密钥文件到期前将其保存，以便在重新安装或恢复软件组件时使用。如丢失密钥文件可在指定网址重复注册操作，重新获取授权密钥文件；重新注册时需输入与第一次注册相同的序列号和相同的客户信息；只可更改邮箱地址。更改邮箱地址后授权密钥文件会发送至新地址。

可使用试用密钥文件了解反病毒软件功能。试用密钥可保证主要反病毒组件的所有功能的运行，但使用期有限。获取试用密钥文件需在网页https://download.drweb.com/demoreq/biz/填写申请表。我公司会对申请进行审核。批准后授权密钥文件压缩文档会发送到用户指定的邮箱。

Dr.Web Enterprise Security Suite授权原则和特点详见**管理员手册**中的第三章、授权。

如何在安装过程中使用授权密钥文件详见安装Dr.Web服务器。

如何在已部署的反病毒网络使用授权密钥文件详见**管理员手册**中的授权管理器。

第四章、开始运行

4.1. 反病毒网络的部署

部署反病毒网络简要说明：

1. 规划反病毒网络结构，使所有应受保护的计算机和移动设备纳入网络。

   选择将作为Dr.Web服务器的计算机。反病毒网络中可以设置几个Dr.Web服务器。这种网络的部署特点详见**管理员手册**中的多台Dr.Web服务器网络的特点。

   > Dr.Web服务器可以安装于任何一台计算机，而不只是执行局域网服务器功能的计算机。对计算机的基本要求见系统要求一节。
   >
   > 在所有受保护计算机，包括局域网服务器，安装同一版本的Dr.Web代理端。区别在于服务器设置中指定有不同的可安装反病毒组件列表。

   安装Dr.Web服务器要求对相应计算机进行一次性访问（实机操作或使用程序远程管理和启用工具）。反病毒工作站的软件一般是由用户自行本地安装，但也可以通过局域网利用Dr.Web安全管理中心进行远程安装。安装完成以后，所有操作都可以由反病毒网络管理员从其计算机进行，不需要访问Dr.Web服务器或工作站。

   在进行反病毒网络规划时建议列出所有有权访问管理中心的责任人，并根据其可以执行的功能设定不同的角色。必须为每一角色创建管理员组。将具体管理员的账户移至相应管理员组就可以实现管理员与角色的对接。如需可以将管理员组（角色）分出级别，设置为多级别体系，可以为每一级别分别设置管理员访问权限。

   管理员组和权限管理详见**管理员手册**中的第6章、反病毒网络管理员

2. 按照网络规划确定网络相应节点应安装适用于何种操作系统的产品。产品详细介绍见供货方案。

   所有产品都可通过Dr.Web Enterprise Security Suite盒装产品购买或通过Doctor Web公司网站 https://download.drweb.com/ 下载。

   > Dr.Web代理端（适用于OS Android、OS Linux、macOS的工作站）可从单机产品软件包安装，之后连接统一保护Dr.Web服务器。代理端设置描述见相应的**用户手册**。

3. 将Dr.Web服务器基本软件安装到选定的一台或几台计算机，安装方法见安装Dr.Web服务器。

   与服务器一起安装Dr.Web安全管理中心。

   默认情况下Dr.Web服务器在安装后自动启动，之后每次重启操作系统时自动启动。

4. 如需请安装并设置代理服务器。详见安装代理服务器。

5. 进行服务器设置和工作站上的反病毒软件包设置必须通过Dr.Web安全管理中心连接服务器。

   > 管理中心和服务器可安装于不同的计算机，只要计算机间有网络连接即可。

   管理中心地址：

   `http://<服务器地址>:9080`

或

`https://<服务器地址>:9081`

其中*<服务器地址>*为安装有Dr.Web服务器的计算机的IP地址或域名。

在身份验证对话窗口输入管理员注册信息。超级管理员默认为：

- 用户名——**admin**。
- 密码：
  - OS Windows下为安装服务器时指定的密码。
  - UNIX家族操作系统下密码是服务器安装过程中自动生成的密码（参见OS UNIX下Dr.Web服务器的安装）。

成功连接服务器后即打开管理中心主窗口（详见**管理员手册**中的Dr.Web安全管理中心）。

6. 进行服务器初始设置（服务器设置详见**管理员手册**中的第9章、Dr.Web服务器设置）：
   a. 在授权管理器添加一个或几个授权密钥并将其分发给相应的组，包括**Everyone**组。如安装服务器时未给出授权密钥，则必须执行此步骤。
   b. 在库常规配置指定将从Dr.Web GUS进行更新的反病毒网络组件。如反病毒网络中有OS Android、OS Linux和macOS工作站，必须下载**Dr.Web企业产品**。

      在库状态更新服务器库中产品。更新可能占用很长时间。需等待更新结束后继续进行设置。

      > 安装的服务器为版本12时库产品**用于Android操作系统的Dr.Web代理端、用于UNIX操作系统的Dr.Web代理端**和**Dr.Web代理服务器**默认情况下只在工作站申请更新这些产品后才会更新。参见**管理员手册**，中的库详细配置。
      >
      > 如果您使用的服务器未接通互联网，而是手动从另一服务器或利用库加载器加载更新，则在安装或更新在库设置中为其启用了**只在接到申请时更新**选项的产品前必须手动将这些产品加载到库中。

   c. 在**管理**→ **Dr.Web服务器**页面为服务器版本介绍。如有新版本，需更新服务器，更新操作介绍见**管理员手册**中的更新Dr.Web服务器和利用备份还原。
   d. 如需，可设置网络连接，更改反病毒网络所有组件交互作用使用的默认网络设置。
   e. 如需可设置服务器管理员列表。可使用管理员外部身份认证。详见**管理员手册**中的第6章、反病毒网络管理员。
   f. 在开始使用反病毒软件前建议改变服务器重要数据备份目录设置（参见**管理员手册**中的Dr.Web服务器日程设置）。备份目录最好设于另一本地磁盘，以减少同时失去服务器软件文件和备份的可能性。
7. 指定工作站反病毒软件设置和配置（组和工作站设置描述参见**管理员手册**中的第7章和第8章）：
   a. 如需可创建工作站用户组。
   b. 设置组**Everyone**和所创建的用户组。包括设置各组可安装组件部分。
8. 将Dr.Web代理端软件安装到工作站。

   在安装文件查看安装代理端可用文件。根据工作站操作系统、是否可以远程安装以及服务器对安装代理端的设置等等选择适合的安装方式。如：

   - 如果用户自行安装反病毒软件，需使用通过管理中心为每一工作站创建的个人安装包。此类型安装包可从管理中心直接发送到用户邮箱。安装后工作站会自动连接到服务器。
   - 如需将反病毒软件安装到同一用户组中的多个工作组，可使用在管理中心创建的组安装包，一份安装包可用于一个组的几个工作站。

- 通过网络安装一个或同时安装几个工作站(仅限Windows操作系统工作站)时需使用网络安装程序。安装通过管理中心来完成。
- 还可以使用Active Directory服务通过网络安装一个或同时安装几个工作站。安装需使用针对带有Active Directory网络的Dr.Web代理端安装程序，此安装程序包含于Dr.Web Enterprise Security Suite软件，但独立于服务器安装程序。
- 如需要减小安装过程中服务器与工作站的通道负载，可使用完整安装程序，以便同时安装代理端和保护组件。
- 在OS Android、OS Linux、macOS工作站可按照常规进行本地安装。也可根据相应配置将已安装的单机产品连接到服务器。



Dr.Web代理端在Windows Server 2016以及更高版本的Windows服务器操作系统上正常运行必须利用组策略手动停用Windows Defender。

9. 代理端安装后会自动连接服务器。反病毒工作站在服务器上的身份验证方式取决于您所选择的策略(参见**管理员手册**中的工作站连接策略)。
   a. 从安装包进行安装且设置为服务器自动确认工作站时工作站在第一次连接服务器时会自动注册，不需要另加确认。
   b. 从安装包进行安装且设置为手动确认时管理员必须手动确认新工作站来完成新工作站在服务器的注册。这时新工作站不会自动连接，而是被列入服务器的新工作站组。
10. 连接服务器并获得设置后，工作站上安装的将是工作站基组基组设置中所指定的反病毒软件包组件。



结束工作站组件安装需重启电脑。

11. 也可在安装后指定工作站反病毒软件设置和配置(参见**管理员手册**中的第8章)。

4.2. 网络连接设置

概述

连接Dr.Web服务器的客户端有：

- Dr.Web代理端。
- Dr.Web代理端安装程序。
- Dr.Web邻居服务器。
- Dr.Web代理服务器。

连接总是由客户端主动建立。

客户端连接服务器可以通过以下方式：

1. 通过直接连接。
   这种方式有很多优点，但并不是在任何情况下都是最佳方式(还有些情况下这种方式不可取)。
2. 通过服务器发现服务。
   默认情况下(如果未直接指定其他方式)客户端使用的正是这一服务。

如果有可能会需要重新设置整个系统，例如需要将 Dr.Web服务器转至另一台计算机或者有必要改变安装有服务器的计算机的IP地址时，需要使用这种连接方式。

3. 使用SRV协议。

   利用这种方式可以按照计算机名称搜索服务器和／或按照DNS服务器SRV记录搜索服务器服务。

设置反病毒网络Dr.Web Enterprise Security Suite使用直接连接时可以关闭服务器发现服务。关闭服务时传输描述（**管理** → **Dr.Web服务器配置** → 网络 → 传输）中的**Multicast**组一栏应为空。

防火墙设置

反病毒网络各组件正常互动要求在所有反病毒网络中的计算机上打开反病毒网络组件所使用的所有端口和接口。

安装服务器时安装程序会自动将服务器的端口和接口添加到OS Windows防火墙排除项。

如除了OS Windows操作系统内设防火墙外还使用其它防火墙，网络管理员应手动进行相应设置。

4.2.1. 直接连接

Dr.Web服务器设置

在服务器设置中应指定接收TCP连接所应监听的地址（参见**附录**中的附录E. 网络地址特点）。

此参数需在服务器设置中的**管理** → **Dr.Web服务器配置** → 网络 → 传输 → **地址**一栏指定。

默认情况下服务器设定"监听"的是：

- **地址**：为空表示使用安装服务器的计算机的*所有网络接口*。
- **端口**：2193——使用端口2193。



端口2193为Dr.Web Enterprise Management Service在IANA注册的端口。

服务器只要"监听"一个所有客户端已知的TCP端口即可保证 Dr.Web Enterprise Security Suite整个系统的正常运行。

Dr.Web代理端设置

安装代理端可以在以下参数明确指明服务器地址（启动Dr.Web服务器的计算机的IP地址或DNS名称）：

```
drwinst /server <服务器地址>
```

安装代理端时建议使用事先已在DNS注册的服务器名称。这样做如果将来Dr.Web服务器安装到另一台计算机，可以简化反病毒网络设置过程。

默认情况下没有给出参数的`drwinst`命令会扫描网络搜索Dr.Web服务器并尝试将代理端与在网络中搜索到的第一个服务器建立连接（使用服务器发现服务的*Multicasting*模式）。

这样代理端将在安装过程中得知Dr.Web服务器地址。

之后可在代理端设置中手动更改服务器地址。

4.2.2. Dr.Web服务器搜索服务

使用这一连接方式时客户端事先不知道服务器地址。在每次建立连接前都在网络中进行服务器搜索。进行搜索时客户端向网络发送广播申请，等待服务器回应其地址。接到回应后与服务器建立连接。

这时服务器应对网络进行"监听"，以便获取客户端的连接申请。

设置这种连接方式有几种途径.最重要的是为客户端指定的服务器搜索方式要与服务器回应部分的设置相符。

Dr.Web Enterprise Security Suite默认情况下使用的是*Multicast over UDP*模式：

1. 服务器在组播组中以服务器设置中的地址注册。
2. 代理端在搜索服务器时第1中指定的组播地址向网络发出组播请求。

默认情况下为服务器进行的监听设定（与直接连接相似）：`udp/231.0.0.1:2193`。

此参数需在服务器设置中的**管理** → **Dr.Web服务器配置** → 网络 → 传输 → **Multicast**组一栏指定。

4.2.3. 使用SRV协议

OS Windows客户端支持客户端网络协议*SRV*（网络格式列于**附录**中的附录E. 网络地址特点）。

实现**通过SRV记录连接服务器的方式**：

1. 安装服务器时在Active Directory域名注册，安装程序将相应的SRV记录载入DNS服务器。

   SRV记录按照RFC2782载入DNS服务器（见https://tools.ietf.org/html/rfc2782）。

2. 申请连接服务器时用户通过`srv`提交申请。

   例如：启动代理端安装程序：

   - 明指服务名称`myservice`：
     ```
     drwinst /server "srv/myservice"
     ```
   - 不明指服务名称。这时将在SRV记录搜索默认名称`drwcs`：
     ```
     drwinst /server "srv/"
     ```
3. 客户端使用SRV协议功能连接服务器。

   如服务器未指明，默认使用的服务名称为`drwcs`。

4.3. 保障安全连接

4.3.1. 流量加密和压缩

加密模式用于保证非安全通道传输的数据的安全，避免重要信息泄露以及加载到受保护工作站的软件被替换。

Dr.Web Enterprise Security Suite反病毒网络使用以下加密手段：

- 电子数字签名（国标 R 34.10-2001）。
- 非对称加密（VKO GOST R 34.10-2001 — RFC 4357）。
- 对称加密（国标28147-89）。
- 哈希加密功能（国标 R 34.11-94）。

Dr.Web Enterprise Security Suite反病毒网络可加密服务器与客户端之间的流量，包括：

- Dr.Web代理端。
- Dr.Web代理端安装程序。
- Dr.Web邻居服务器。
- Dr.Web代理服务器。

由于组件间特别是服务器之间可能会出现很大的流量，反病毒网络可设置对此流量进行压缩。设置压缩策略和不同客户端间的设置兼容性与加密设置相同。

设置兼容策略

加密和压缩使用策略在反病毒网络每一组件分别设置，同时其它组件的设置应与服务器的设置相符。

在设置服务器和客户端加密和压缩策略时应注意有些设置会产生冲突，导致服务器和客户端失去连接。

表 4-1 中何种设置下服务器与客户端间的连接为加密/压缩（+），何种设置下为不加密/不压缩（–），哪些设置会产生冲突（错误）。

表4-1. 加密和压缩策略设置兼容

客户端设置	服务器设置		
	是	可能	否
是	+	+	错误
可能	+	+	–
否	错误	–	–



如果计算机性能接近所安装组件的最低要求，流量加密会显著增加其计算负荷。如果没有额外安全保证的需求，可以不使用加密模式。

取消加密时应依次将服务器和组件转为**可能**模式，以免服务器-客户端间发生冲突。

使用压缩会减小流量，但相比加密，要占用更多内存，会更大程度地增加计算机的计算负荷。

通过Dr.Web代理服务器连接

客户端通过Dr.Web代理服务器连接服务器时必须考虑所有三个节点的加密和压缩设置。这时：

- 服务器和代理服务器（这时作为客户端）的设置一个按照表4-1匹配。
- 客户端和代理服务器（这时作为服务器）的设置一个按照表4-1匹配。

是否可以通过代理服务器取决于服务器和客户端相应版本所支持的加密技术：

- 如果服务器和客户端支持12.0版本中使用的TLS加密，则只需执行上面描述的条件就可以建立连接。
- 如果有一个组件不支持TLS加密：在服务器和/或客户端安装的是使用国标加密的版本10或更早版本，则需要按照表4-2进行补充检查。

表4-2. 使用代理服务器时加密和压缩策略设置兼容

与客户端的连接设置	**与服务器的连接设置**			
	无	压缩	**加密**	**全部**
无	一般模式	一般模式	错误	错误
压缩	一般模式	一般模式	错误	错误
加密	错误	错误	**透明模式**	错误
全部	错误	错误	错误	**透明模式**

标志说明

与服务器和客户端的连接设置	
无	压缩和加密都不支持。
压缩	**只支持**压缩。
加密	**只支持**加密。
全部	压缩和加密都支持。
连接结果	
一般模式	**已建立的**连接意味着以一般模式运行，处理指令并进行缓存。

透明模式	已建立的连接意味着以透明模式运行，不处理指令，不进行缓存。选择最低的加密协议版本：如果有一个客户端（服务器或代理端）为版本11，而另一个是版本10，则建立版本10中使用的加密。
错误	代理服务器与服务器和客户端的连接将中断

这样，如果服务器和代理端版本不同：一个是版本11，另一个是版本10或更低，则通过代理服务器建立连接应用以下限制：

- 在代理服务器进行缓存只能是在与服务器和客户端的连接都不使用加密的情况下。
- 使用加密只能是与服务器和客户端的连接都使用加密且压缩参数相同（两个连接都有压缩或都没有压缩）。

在Dr.Web服务器设置加密和压缩

设置服务器压缩和加密的操作

1. 在管理中心主菜单选择**管理**。
2. 在打开的窗口选择控制菜单中的**Dr.Web服务器配置**。
3. 在网络 → 传输标签的**加密**和压缩下拉列表中选择以下一种方案：
   - **是**——同所有客户端间的流量都必须加密（或压缩）（如安装服务器时未另行设置，此方案为加密默认设置）。
   - **可能**——如客户端的设置不禁止加密（或压缩），则与这些组件间的流量将进行加密（或压缩）。
   - **否** ——不支持加密（或压缩）（如安装服务器时未另行设置，此方案为压缩默认设置）。



在服务器端设置加密和压缩时许注意将和此服务器连接的客户端的特点。并非所有客户端都支持流量加和压缩。

在Dr.Web代理服务器设置加密和压缩

统一为代理服务器设置加密和压缩



如果代理服务器未连接Dr.Web服务器，因而不能远程进行设置管理。需按照中的将代理服务器连接到Dr.Web服务器的描述设置连接。

1. 为代理服务器的控制服务器打开管理中心。
2. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击需编辑其设置的代理服务器的名称，如果代理服务器从基组继承设置，则点击基组名称。
3. 在打开的控制菜单选择**Dr.Web代理服务器**。打开设置选项。
4. 打开监**听**标签。
5. 在**与客户端的连接参数**的加密和压缩下拉列表中选择代理服务器和其所服务的客户端间流量的加密和压缩模式，包括代理端和代理端安装程序。

6. 在**在与Dr.Web服务器的连接参数**指定向其重定向流量的服务器列表。在表中选择需要的服务器后点击这一部分工具面板的按钮，编辑与所选Dr.Web服务器的连接参数。在打开的窗口的**加密**和压缩下拉列表选择代理服务器与所选服务器间流量的加密和压缩模式。
7. 点击**保存**按钮保存指定的设置。

为**代理服务器本地设置加密和**压缩

> 如果代理服务器连接Dr.Web控制服务器，可进行远程设置，则将按照从服务器获取的设置重写代理服务器的配置文件。这种情况下必须从服务器远程指定设置或停用从这一服务器接收配置。
>
> 配置文件`drwcsd-proxy.conf`描述见**附录**的附录G4。

1. 在安装代理服务器的电脑端口配置文件`drwcsd-proxy.conf`。
2. 点击与客户端和服务器连接的压缩和加密设置。
3. 重启代理服务器：
   - OS Windows：
     - 如果代理服务器是作为OS Windows服务启动，则利用系统工具重启服务。
     - 如果代理服务器是在控制台启动，重启需点击CTRL+BREAK。
   - UNIX家族操作系统：
     - 将信号`SIGHUP`发送给代理服务器守护进程。
     - 需执行以下命令：

       OS Linux：

       ```
       /etc/init.d/dwcp_proxy restart
       ```

       OS FreeBSD：

       ```
       /usr/local/etc/rc.d/dwcp_proxy restart
       ```

为工作站设置加密和压缩

统一为**工作站**设置**加密和**压缩

1. 在管理中心主菜单选择**反病毒网络**，在打开窗口的分层列表中点击工作站或组的名称。
2. 在打开的控制菜单选择**连接参数**。
3. 在**常规**标签压缩**模式**和**加密模式**下拉列表中选择以下一种方案：
   - **是**——一定加密(或压缩)与服务器间的流量。
   - **可能**——如服务器的设置不禁止加密(或压缩)，则与服务器的流量将进行加密(或压缩)。
   - **否**——不支持加密(或压缩)。
4. 点击**保存**。
5. 设置传至工作站后立即生效。如更改设置时工作站离线，则更改会在工作站再次连接服务器时立即传至工作站。

用于Windows操作系统的Dr.Web代理端

可在安装代理端时设置加密和压缩：

- 从管理中心进行远程安装时直接在网络**安装**的设置中指定加密和压缩模式。
- 进行本地安装时图形安装程序不可更改加密和压缩模式，但可在启动安装程序时利用命令行参数进行设置（参见**附**录中的H1. 网络安装程序）。

完成代理端安装后不可在工作站本地更改加密和压缩模式。默认模式设置为**可能**（如安装过程中未另行指定），也就是说是否加密和压缩取决于服务器端的设置。但可以通过管理中心更改代理端的设置（见上）。

用于Android操作系统的Dr.Web反病毒软件

反病毒软件Dr.Web for Android不支持加密，也不支持压缩。如果服务器端或代理服务器端（如通过代理服务器建立连接）压缩和/或加密的设置为**是**，将无法连接服务器。

用于Linux操作系统的Dr.Web反病毒软件

安装反病毒软件是不可更改加密和压缩模式。默认模式为**可能**。

完成反病毒软件安装后只可通过控制台模式更改工作站的加密和压缩设置。控制台模式介绍和相应的命令行参数见**Dr.Web for Linux用户手册**。

也可通过管理中心更改工作站设置（见上）。

用于macOS的Dr.Web反病毒软件

完成代理端安装后不可再工作站本地更改加密和压缩模式。默认模式设置为**可能**，也就是说是否加密和压缩取决于服务器端的设置。

也可通过管理中心更改工作站设置（见上）。

4.3.2. 安全连接保障工具

安装Dr.Web服务器时创建以下保障反病毒网络各组件间安全连接的工具：

1. **服务器加密私钥**`drwcsd.pri`。

   保存在服务器，不分发给反病毒网络其他组件。

   如丢失私钥需手动恢复反病毒网络各组件间的连接（创建所有密钥和证书并将其分发到网络所有组件）。

   以下情况使用私钥：

   a) 创建公钥和证书。

   加密公钥和证书在安装服务器过程中自动从私钥创建。私钥可以是新创建的，也可以为已有私钥（如上一服务器私钥）可随时使用服务器工具`drwsign`创建加密密钥和证书（参见 **附**录中的 H7.1.数字密钥和证书生成工具）。

公钥和证书介绍见下。

b) 服务器验证。

远程客户端进行服务器验证使用的是电子数字签名(每次连接进行一次)。

服务器使用私钥为通知进行数字签名后将通知发送给客户端。客户端利用证书检查通知签名。

c) 数据解密。

服务器和客户端间流量加密时客户端发送给服务器的数据利用私钥在服务器解密。

2. 服务器加密公钥`drwcsd.pub`**。**

反病毒网络所有组件均可访问。公钥从私钥创建(见上)。从同一私钥每次生成的公钥相同。

从服务器版本11开始公钥用于连接老版本的客户端。其他功能由证书取代,证书中包含加密公钥。

3. 服务器证书`drwcsd-certificate.pem`**。**

反病毒网络所有组件均可访问。证书中包含加密公钥。证书从私钥创建(见上)。从同一私钥每次生成的新的证书。

连接服务器的客户端与具体证书对应,因此如某客户端丢失证书,则只有当网络中还有另一组件也使用同一证书的情况下才有可能找回证书:可从服务器或另一客户端将证书复制到丢失证书的客户端。

以下情况使用证书:

a) 服务器验证。

远程客户端进行服务器验证使用的是电子数字签名(每次连接进行一次)。

服务器使用私钥为通知进行数字签名后将通知发送给客户端。客户端利用证书检查通知签名(具体是利用证书中包含的公钥)。之前的服务器版本是直接利用公钥。

要求客户端具备来自其要连接的服务器的一个或几个可信任证书。

b) 数据解密。

服务器和客户端间流量加密时客户端发送给服务器的数据利用公钥在客户端解密。

c) 实现服务器与远程客户端之间的TLS对话。

d) 代理服务器验证。

远程客户端进行代理服务器验证使用的是电子数字签名(每次连接进行一次)。

代理服务器使用Dr.Web服务器私钥和证书为自己的证书签名。信任Dr.Web服务器证书的客户端会自动信任使用这一证书签名的证书。

4. Web服务器私钥。

保存在服务器,不分发给反病毒网络其他组件。详细介绍见下。

5. Web服务器证书。

反病毒网络所有组件均可访问。

用于实现Web服务器与浏览器之间的TLS对话(按照HTTPS)。

以Web服务器私钥为基础安装服务器时生成自签名证书,由于此证书不是知名证书中心发布,因此浏览器不会接受。

要使用受保护的连接(HTTPS),需执行以下一种操作:

- 将自签名证书添加到所有工作站和打开管理中心的浏览器的可信任证书或排除项。
- 获取由知名证书中心发布的证书。

4.3.3. 将客户端连接到Dr.Web服务器

客户端连接到Dr.Web服务器要求客户端必须具备服务器证书，不论服务器和客户端直接的流量是否加密。

可连接Dr.Web服务器的客户端有：

- **Dr.Web代理端。**

  连接Dr.Web服务器以便在统一管理模式下运行代理端要求工作站具备来自代理端连接的服务器的一个或几个可信任证书。

  安装时使用的证书以及通过统一设置从服务器获得的证书处于注册表，但不使用证书文件本身。

  可以利用命令行参数将唯一一份证书文件添加到代理端安装目录（而非注册表）和证书总表。使用这一证书在统一设置出现错误时也可连接到服务器。

  没有证书或证书无效时代理端无法连接到服务器，但会继续运行，并可以移动模式更新，如允许工作站在此模式下运行。

- **Dr.Web代理端安装程序。**

  在工作站安装代理端时所选安装文件应同时具备服务器证书。

  启动在管理中心创建的安装包时，安装包包含证书，不需要另行指定证书文件。

  安装代理端时证书数据记录到注册表，之后不再使用证书文件本身。

  没有证书或证书无效时安装程序不能安装代理端（包括所有类型代理端安装文件）。

- **Dr.Web邻居服务器。**

  设置版本11或更高版本的邻居服务器间连接时必须在每一服务器指定其连接的服务器的证书（参见**管理员手册**中的设置Dr.Web服务器间连接）。

  任何一个证书不存在或无效都会导致无法建立服务器间连接。

- **Dr.Web代理服务器。**

  代理服务器连接Dr.Web服务器并可通过管理中心进行远程配置要求安装代理服务器的工作站上有证书。这时代理服务器还支持加密。

  没有证书的情况下代理服务器会继续运行，但无法进行远程管理，也不支持加密和缓存。



原来使用公钥的老版本反病毒网络正常更新为使用证书的新版本不需要进行任何其他操作。

不建议将版本11服务器提高的代理端连接版本10的服务器或将版本10服务器提高的代理端连接版本11的服务器。

4.4. Dr.Web Enterprise Security Suite与Active Directory的集成

如果受保护的局域网中使用Active Directory，可此服务与Dr.Web Enterprise Security Suite集成。



下面介绍的所有方法各自独立，可单独使用，也可结合使用。

Dr.Web Enterprise Security Suite与Active Directory的集成基于以下方法：

1. **在Active Directory域名注册Dr.Web服务器，以便使用SRV协议访问服务器**

   安装Dr.Web服务器时可以利用安装器在Active Directory域中注册服务器。在DNS服务器注册过程中会创建对应Dr.Web服务器的SRV记录。之后客户端可通过此SRV记录连接Dr.Web服务器。

   详见OS Windows下Dr.Web服务器的安装和使用SRV协议。

2. **将反病毒网络结构与Active Directory域同步**

   可设置反病毒网络结构与Active Directory域中工作站自动同步。此时Active Directory计算机容器转变为反病毒网络工作站组。

   操作是在服务器日程启用任务**与Active Directory同步**。管理员可利用Dr.Web服务器任务计划器自行创建此任务。

   详见**管理员手册**Dr.Web服务器日程设置。

3. **Active Directory用户作为管理员在Dr.Web服务器进行身份验证**

   可以使用Active Directory账户在Dr.Web服务器进行身份验证后管理反病毒网络。可使用以下一种方式：

   - LDAP/AD身份验证。适用于所有支持的操作系统的服务器。通过管理中心按照相应Active Directory属性为用户设置服务器访问权限。不需直接访问域控制器和Active Directory设备，不需在Active Directory端进行设置。
   - Microsoft Active Directory。仅适用于纳入目的域的OS Windows服务器。直接在Active Directory设备设置有服务器访问权限的用户和用户组。需利用补充工具进行初始设置。数据包`drweb-<数据包版本>-<编号>-esuite-modify-ad-schema-<操作系统版本>.exe`和`drweb-<数据包版本>-<编号>-esuite-aduac-<操作系统版本>.msi`包含于**Dr.Web企业产品**的服务器库。

   选择哪种方式取决于Dr.Web服务器操作系统和有访问权限的用户的设置方法。

   详见**管理员手册**管理员身份验证。

4. **在Active Directory域工作站远程安装Dr.Web代理端**

   可在Active Directory域工作站远程安装Dr.Web代理端。操作是：

   a) 借助用于Active Directory的专门代理端安装器在目标共享资源进行管理员安装。数据包`drweb-<数据包版本>-<编号>-esuite-agent-activedirectory.msi`包含于**Dr.Web企业产品**的服务器库。

   b) 设置Active Directory相应策略，以便将数据包自动安装到域内工作站。

详见 中的使用Active Directory服务安装Dr.Web代理端。

5. **在Active Directory域搜索工作站**

   可利用网络搜索已在Active Directory域中搜索工作站。搜索是可以确认找到的工作站是否已安装有Dr.Web，如未安装，则通过管理中心远程安装代理端。

   可将此方法与第4部分介绍的利用Active Directory策略自动安装数据包的方法一同使用。

   详见**管理员手册**的网络搜索仪。

6. **在Active Directory域搜索用户**

   可在Active Directory搜索用户并为其创建用户模式，提供办公控制和应用程序监控的更多设置。

   详见**Windows工作站管理手册**。

第五章、安装Dr.Web Enterprise Security Suite组件

开始安装Dr.Web Enterprise Security Suite组件前请阅读反病毒网络的部署。

5.1. 安装Dr.Web服务器

部署反病毒网络的第一步是安装Dr.Web 服务器。在成功安装服务器以前无法进行反病毒网络其它组件的安装。

Dr.Web服务器安装过程取决于是服务器版本(用于OS Windows还是用于OS UNIX家族)。

安装时设置的所有参数反病毒网络管理员在今后服务器运行过程中都可以进行更改。

如果已安装了服务器软件，请查看 OS Windows下Dr.Web服务器的更新或UNIX家族操作系统Dr.Web服务器的更新 。

如果在安装服务器软件前对先前安装的服务器进行了删除，在安装过程中将删除库的内容并安装库的新版本。如果由于某种运行保留了原来的库，则必须在安装新版服务器前手动删除库的所有内容，并在安装服务器后对库进行全部更新。

服务器所在文件夹名称所使用的语言应与Windows操作系统语言设置中为不使用unicode的软件所指定的语言。如不相符则无法安装服务器。

例外是安装文件夹名称要使用英文。

安装Dr.Web 服务器时会同时自动安装Dr.Web安全管理中心，管理中心将用于反病毒网络管理和服务器的设置。

默认情况下OS Windows Dr.Web服务器安装结束后会自动启动，UNIX家族操作系统的版本需手动启动。

5.1.1. OS Windows下Dr.Web服务器的安装

以下为用于OS Windows的Dr.Web服务器的安装操作。

在开始安装Dr.Web服务器前请留意以下信息：

程序文件和安装过程中需要的其他文件应处于进行服务器软件安装的计算机的本地硬盘。其访问权限应设置为可由 **LOCALSYSTEM**用户进行访问。

安装Dr.Web服务器要求用户具备本机的管理员权限。

Dr.Web服务器安装后必须更新 Dr.Web Enterprise Security Suite的所有组件(参见**管理员手册**中的手动更新Dr.Web服务器库)。

如使用外设数据库必须事先建立数据库并设置相应的驱动程序(参见**附录**中的附录B. DBMS使用设置。DBMS驱动程序参数)。

图 5-1为使用安装程序进行Dr.Web 服务器安装的过程示意图。图中分出的各步骤的详细介绍见下。

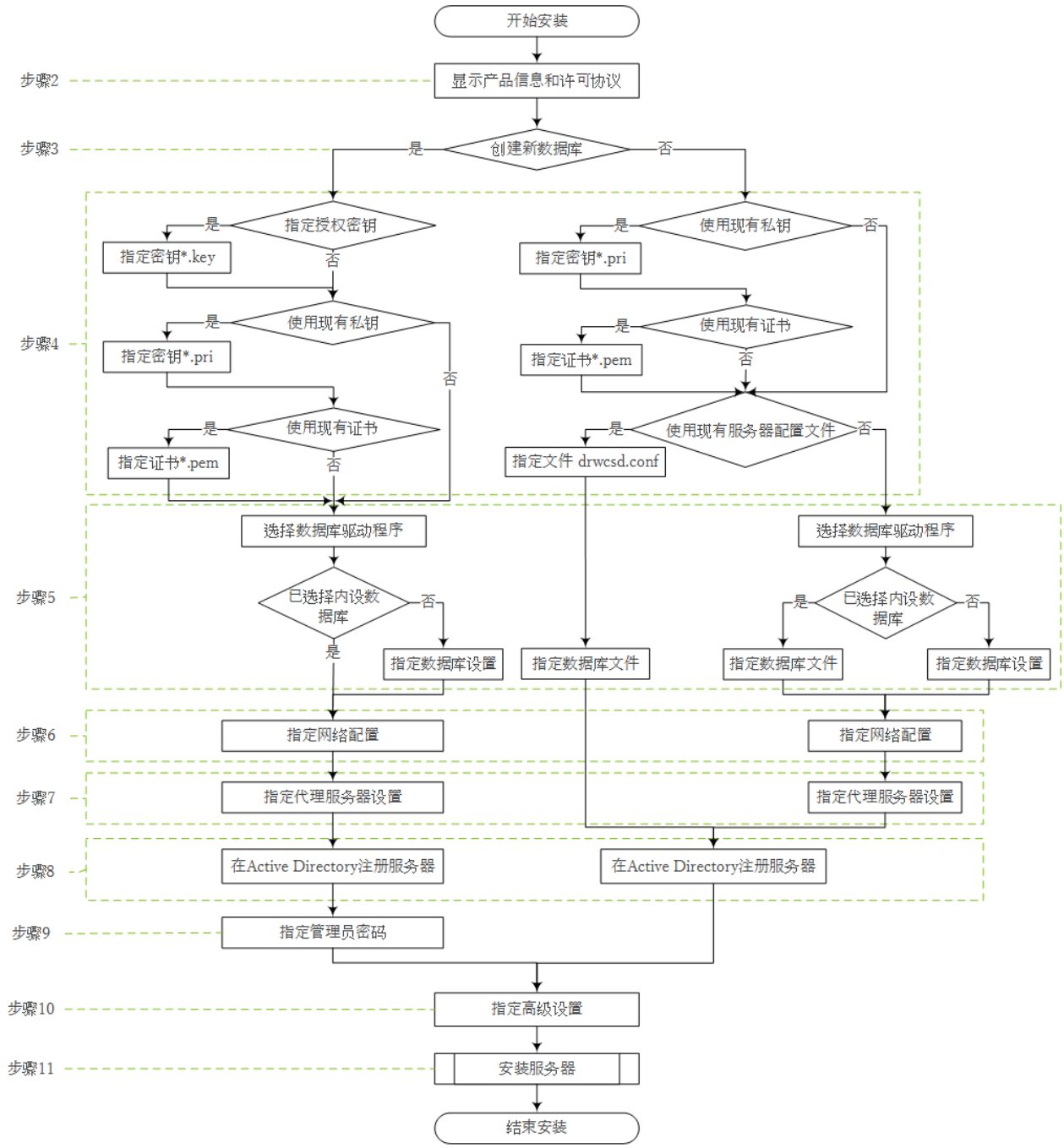


图 **5-1。Dr.Web服务器安装过程示意图(点击示意图可转至步骤文字说明)**

Windows 操作系统计算机Dr.Web服务器安装步骤

1. 启动程序文件。

> 安装程序默认语言为操作系统语言。如需可在安装任一帮助点击安装程序右上角的相应选项更改语言。

2. 打开产品信息及许可协议条款的窗口。了解许可协议条件继续安装需选择**我接受许可协议的条款**并点击**下一步**按钮。
3. 在下一窗口现在反病毒网络使用的数据库：
   - **创建新数据库**——用于创建新的反病毒网络。
   - **使用现有数据库**——如果要保留上一次安装的服务器数据库。数据库文件可稍后指定（见步骤**5**）。
4. 在下一个窗口需进行数据库设置。

   a) 如果在步骤**3**选择的是**创建新数据库**，需在**新数据库参数**窗口指定以下设置：

   - 选项 **指定授权密钥**用于在服务器安装过程中指定Dr.Web代理端授权密钥文件。
     - 如取消勾选，服务器安装过程中不需要指定代理端授权密钥。这种情况下授权密钥应在服务器安装后通过授权管理器添加。
     - 如勾选此项作为需在相应输入栏指定代理端授权密钥路径。
   - 选项**使用现有加密私钥**用于使用现有加密密钥，如上次安装的服务器加密密钥。
     - 如果是第一次安装服务器，需取消对**使用现有加密私钥**的勾选。新的加密密钥和证书将在安装过程中自动生成。
     - 如果是为现有反病毒网络安装服务器，请勾选**使用现有加密私钥**，然后在相应输入栏指定私钥文件路径。之后将自动创建加密公钥文件（公钥内容将与原公钥内容一致）和证书（从同一私钥每次生成新的证书）。
     - 如果是为现有反病毒网络安装服务器，并使用现有加密私钥，请勾选**使用现有证书**，以便指示之前使用的证书文件。这样已安装的代理端就会连接到新安装的服务器，因为连接服务器的客户端与一定证书捆绑（从同一私钥每次生成新的证书）。如不进行上述操作，安装完成后需要将新的证书拷贝到所有先前已安装了Dr.Web代理端的工作站。
     - 如提取加密公钥出错，需手动在打开的输入栏**加密公钥**指定相应加密公钥的路径。

   为了解产品起见可以使用试用密钥文件。点击**申请试用密钥**后转至Doctor Web公司网站获取试用密钥文件（参见试用密钥文件）。

   b) 如果在步骤**3**选择的是**使用现有数据库**，需在现**有数据库参数**窗口指定以下设置：

   - 选项**使用现有配置文件**用于指定服务器设置。
     - 如取消勾选，将使用默认设置已创建服务器配置文件。
     - 如勾选此项作为需在相应输入栏指定服务器配置文件路径。
   - 选项**使用现有加密私钥**用于使用现有加密密钥，如上次安装的服务器加密密钥。
     - 如果是第一次安装服务器，需取消对**使用现有加密私钥**的勾选。新的加密密钥和证书将在安装过程中自动生成。
     - 如果是为现有反病毒网络安装服务器，请勾选**使用现有加密私钥**，然后在相应输入栏指定私钥文件路径。之后将自动创建加密公钥文件（公钥内容将与原公钥内容一致）和证书（从同一私钥每次生成新的证书）。

- 如果是为现有反病毒网络安装服务器，并使用现有加密私钥，请勾选**使用现有**证书，以便指示之前使用的证书文件。这样已安装的代理端就会连接到新安装的服务器，因为连接服务器的客户端与一定证书捆绑（从同一私钥每次生成新的证书）。如不进行上述操作，安装完成后需要将新的证书拷贝到所有先前已安装了Dr.Web代理端的工作站。
- 如提取加密公钥出错，需手动在打开的输入栏**加密公钥**指定相应加密公钥的路径。

为了解产品起见可以使用试用密钥文件。点击**申请试用密钥**后转至Doctor Web公司网站获取试用密钥文件（参见试用密钥文件）。

5. 在**数据**库驱动**程序**窗口对所使用的数据库进行参数设置，参数取决于步骤**3**所选数据库类型以及步骤**4**是否给出服务器配置文件。
   - 如果在步骤**3**选择的是创**建新数据**库，或为**使用**现**有数据**库在步骤**4**给出服务器配置文件路径，需选择驱动**程序**。这时：
     - **SQLite**（**内**设**数据**库）要求使用Dr.Web服务器内部工具。不需要指定补充参数。
     - 其他方案意味着使用相应的外设数据库.这时必须指定访问数据库的参数。DBMS参数设置详见附录（参见**附**录中的附录B. DBMS使用设置。DBMS驱动程序参数）。
   - 如果在步骤**3**选择的是**使用**现**有数据**库，并在步骤**4**给出服务器配置文件路径，需选择按照此服务器配置文件使用的数据库文件路径。
6. 如果在步骤**3**选择的是创**建新数据**库，或**使用**现**有数据**库在步骤**4**没有给出服务器配置文件路径，会打开**网络配置**窗口。在此窗口设置服务器运行使用的网络协议（只允许指定一个协议；补充协议可在以后设置）。

   指定预设网络设置需在下拉列表中选择以下一种方式：
   - 标**准配置**为使用基于服务器发现服务的默认设置。
   - **受限配置**限制服务器运行只使用内网接口——127.0.0.1。在这种设置下只能通过与服务器安装在同一计算机的管理中心对服务器进行管理，也只有在同一计算机启动的代理端才能接通服务器。在完成服务器设置调试后可以更改这一网络设置。
   - **自定**义**配置**意味着更改以下预设设置：
     - 在**接口**和**端口**两栏输入连接服务器的相应值。默认情况下接口设置为0.0.0.0，这意味着可通过所有接口访问服务器。

   默认使用端口2193。

   地址以网络格式输入，网络格式列于**附**录中的附录E. 网络地址特点。

     - 如需限制对服务器的本地访问，请勾选**限制**访问**Dr.Web服务器**，这样就会禁止对代理端安装程序、代理端以及其它服务器（如果已利用Dr.Web Enterprise Security Suite部署了反病毒网络）的访问。这些设置以后可以进行更改，通过管理中心菜单中**管理**一项的**Dr.Web服务器配置**选项中的**模**块标签。
     - 勾选**服务器**发现**服**务后，服务器会对其它服务器按照下面相应输入栏指定的IP地址和服务器名称进行的广播和多播请求做出回应。
7. 如果在步骤**3**选择的是创**建新数据**库，或为**使用**现**有数据**库在步骤**4**没有给出服务器配置文件路径，打开**代理服**务**器**窗口，需设置使用代理服务器连接服务器的参数：

   使用代理服务器连接服务器需勾选**使用代理服**务**器**。

   使用代理服务**器**这一项只有在服务器安装目录中没有上次安装的配置文件时才可供勾选。

指定下列代理服务器连接参数：

- **代理服务器地址**——代理服务器IP地址或DNS名称（必填项），
- **用户名**、**密码**——如果代理服务器支持登录，需指定代理服务器的登录用户名和密码。
- 如果代理服务器支持登录连接，在**登录方式**下拉列表选择代理服务器登录方式。

8. 如果安装服务器的计算机在Active Directory域中，则在下一查看会建议在Active Directory域名注册服务器。在Active Directory注册过程中DNS服务器创建对应Dr.Web服务器的SRV记录。之后客户端可通过此SRV记录连接Dr.Web服务器。

   注册需给出以下参数：

   - 勾选**将Dr.Web服务器在Active Directory注册**。
   - 在**域名**指定注册服务器的Active Directory域名名称。如不指定，则使用注册了安装服务器的计算机的域名。
   - 在**用户名**和**密码**两栏指定Active Directory域管理员账户。

9. 如果在步骤**3**选择的是创**建新数据**库，打开**管理**员**密**码窗口。需在此窗口指定反病毒网络管理员密码，密码默认使用注册用户名**admin**，以反病毒网络全权管理员权限创建。

10. 在下一窗口安装向导通知已准备安装服务器。必要时可设置高级参数。操作是点击窗口下方的**高级参数**后给出以下设置：

    - 在**常**规标签：
      - 在**Dr.Web安全管理中心界面**语言下拉列表选择 Dr.Web安全管理中心界面默认语言。
      - 在**Dr.Web代理端界面**语言下拉列表选择Dr.Web代理端界面和工作站反病毒软件包组件的默认语言。
      - 勾选**将Dr.Web代理端安装目**录设为**共享**后更改代理端安装文件夹系统共享资源名称和使用模式（默认情况下设定为隐藏共享资源名称）。
      - 勾选**完成安装后启**动**Dr.Web服**务**器**后会在安装完成后自动启动服务器。
      - 勾选**完成安装后更新**库后会在完成服务器安装后立即自动更新库。
      - 勾选**向Doctor Web公司**发**送**统计**信息**后允许将病毒事件统计信息发送给Doctor Web公司。
    - 在**路径**标签：
      - **Dr.Web服务器安装目**录一栏指定进行服务器安装的文件夹。可点击浏览按钮并选择所需文件夹替代默认文件夹。
      - **Dr.Web服务器备份目**录一栏指定按照服务器日程进行服务器重要数据备份的文件夹。可点击浏览按钮并选择所需文件夹替代默认文件夹。
    - 在**日志**标签可设置服务器安装和运行日志。

    结束高级设置后点击**确定**按钮接受更改，如未作任何更改或要取消所作的更改需点击**取消**按钮。

11. 点击**安装**以开始安装进程。接下来的安装过程不再需要用户的参与。

12. 安装结束后请点击**完成**。

通常利用服务器外设界面管理中心来管理Dr.Web服务器。

安装服务器时，Windows操作系统主菜单**程序**出现文件夹**Dr.Web Server**，包含以下对服务器进行设置和基本管理的元素：

- 文件夹**服务器管理**含有服务器启动、重启和结束服务器运行的指令，以及日志设置指令和服务器其它指令，详见**附**录中的H3. Dr.Web服务器。

- **Web界面**选项——用于打开管理中心并连接安装于本机的服务器(使用地址 http://localhost:9080)。
- **帮助文档**选项——用于打开HTML格式的管理员手册文档。

服务器安装目录结构参见**管理员手册**中的Dr.Web服务器。

5.1.2. UNIX家族操作系统Dr.Web服务器的安装

所有安装操作都应从控制台使用超级管理员(**root**)账户进行。

安装UNIX®家族操作系统Dr.Web服务器

1. 启动服务器软件包的安装需完成以下命令:

   ./<*软件版本*>.tar.gz.run

   可使用命令行参数启动安装包。命令行参数参见**附录**中的H6. UNIX家族操作系统Dr.Web服务器安装程序。

   反病毒网络管理员用户名默认为**admin**。

2. 显示许可协议文本。继续安装,必须接受许可协议。
3. 备份目录设定提示中可指定目录,或确认在默认目录/var/tmp/drwcs进行备份。
4. 如在系统中发现补充软件在删除(extra),将提示在安装服务器软件包前需删除补充软件。不进行删除无法继续进行安装。
5. 下一步将安装软件,在安装过程中安装程序会要求您以管理员名义确认操作。
6. 安装过程中为主管理员生成随机密码。结束安装后此密码通过控制台导出到服务器安装结果。

   创建的管理员密码保存到数据库。如需可使用外设数据库管理工具或内设数据库工具drwidbsh查看此密码(详见**附录**中的恢复Dr.Web Enterprise Security Suite管理员密码)。

   FreeBSD操作系统下软件安装过程中创建rc-脚本/usr/local/etc/rc.d/drwcsd。

   请使用以下命令:

   - /usr/local/etc/rc.d/drwcsd stop——用于手动停止服务器;
   - /usr/local/etc/rc.d/drwcsd start——用于手动启动服务器。

   需要注意的是,在服务器安装过程中无需指定授权密钥。授权密钥应在服务器安装后通过授权管理器添加。

设置Astra Linux版本1.6以便使用封闭软件环境模式安装Dr.Web服务器

在使用封闭软件环境模式的Astra Linux版本1.6安装Dr.Web服务器是可能因Dr.Web服务器加密公钥未列入可信任密钥列表而出现拒绝启动安装程序的情况。这时需预先对封闭软件环境模式进行设置，之后再次启动安装程序。

预设置封闭软件环境模式

1. 如之前未进行安装，请从操作系统安装盘安装astra-digsig-oldkeys。
2. 将Dr.Web服务器加密公钥加入目录/etc/digsig/keys/legacy/keys（如无此目录，需创建）。
3. 执行以下命令：

```
# update-initramfs -k all -u
```

4. 重启系统。

5.2. 安装Dr.Web代理端



用户安装Dr.Web代理端应由具有该计算机管理员权限。

如果工作站上已安装有反病毒产品，则在进行新的安装前必须删除原来的反病毒产品。

Dr.Web代理端在Windows Server 2016以及更高版本的Windows服务器操作系统上正常运行必须利用组策略手动停用Windows Defender。

Dr.Web代理端可利用下列一种方式安装到工作站：

1. 本地方式：

   用户直接在用户计算机或移动设备上进行本地安装，用户和管理员均可执行。

2. 远程方式：

   远程安装仅针对OS Windows工作站通过局域网在管理中心进行。由反病毒网络管理员执行。不需要用户的参与。

在安装有Dr.Web单机反病毒产品的OS Windows工作站进行Dr.Web代理端的覆盖安装

如OS Windows工作站安装有Dr.Web单机产品版本7/8/9/10/11，按照以下方式安装Dr.Web Enterprise Security Suite版本12.0的代理端：

- 在安装有7.0/8.0/9.0/9.1/10.0/11.0/11.5版本单机产品的工作站以GUI模式运行代理端安装程序或安装包时，会启动已安装产品的安装程序。随后提示用户需输入确认码确认删除产品。重启操作系统后将运行GUI版本安装程序，安装Dr.Web Enterprise Security Suite版本12.0的代理端。
- 以背景模式在安装有7.0/8.0/9.0/9.1/10.0/11.0/11.5版本单机产品的工作站启动代理端安装程序时不会执行任何操作。远程安装时安装程序将之前安装的单机产品版本信息返给管理中心。此时需以任一方式手动删除单机产品并安装Dr.Web Enterprise Security Suite 12.0版本的代理端。

- 在安装有12.0版本单机产品的工作站上本地或远程启动代理端安装程序时都会将已安装的产品从单机模式转为统一保护模式。连接服务器并成功登录后，可获取更新、新设置及可安装组件列表，安装某些组件可能需要重启。

在局域网服务器和群集计算机安装Dr.Web代理端时必须注意：

- 在局域网作为终端服务器的计算机（OS Windows安装有 **Terminal Services**服务），为保证在代理端用户终端会话时的运行，建议利用OS Windows**控制面板**上的添加和删除程序向导来进行代理端的本地安装。这种情况下进行远程安装有可能导致Remote Desktop协议运行出错。
- 不建议在执行重要网络功能的服务器（域控制器、授权分发服务器等等）安装组件SpIDer Gate、办公控制、SpIDer Mail和Dr.Web防火墙，以免网络服务与Dr.Web反病毒软件内部组件可能发生冲突。
- 代理端群集安装应在群集每一节点分别进行。
- 代理端和反病毒软件包组件在群集节点的运行原则与在局域网一般服务器的运行原则相同，因此不建议在群集节点安装SpIDer Gate、SpIDer Mail和Dr.Web Firewall。
- 如果对群集仲裁资源的访问有严格限制，建议将仲裁资源列入监视器SpIDer Guard的排除项，只定期按日程或手动启用扫描仪进行检查。

5.2.1. 安装文件

安装包

个人安装包

在工作站创建新的用户账户时管理中心就会生成一个用于安装Dr.Web代理端的个人安装包。个人安装包包含Dr.Web代理端安装程序、Dr.Web服务器连接参数及工作站登录Dr.Web服务器参数。

可谓Dr.Web Enterprise Security Suite支持的所有操作系统的工作站提供代理端个人安装包。在管理中心以代理端安装程序为基础生成个人安装包。个人安装包包含服务器连接参数和工作站登录服务器参数。

> 获取非OS Windows操作系统个人安装包，需安装Dr.Web服务器后从全球更新系统将**Dr.Web企业产品**加载到库。
>
> 使用服务器库的详细信息参见**管理员手册**中的Dr.Web服务器库的管理。

可以在以下情况使用工作站Dr.Web代理端个人安装包下载链接：

1. 创建新工作站后即可使用（参见创建工作站新账户一节中的步骤**11**）。
2. 在工作站创建后：
   - 在工作站属性中，
   - 在分层列表选择工作站后在**所选对象**一项。

组安装包

代理端组安装包在管理中心生成，用于安装某一用户组的工作站。这时时从同一个组安装包将代理端安装到同一操作系统的工作站。

组安装包中包含代理端安装程序、服务器连接参数以及安装代理端后工作站所属用户组的识别码和密码。但组安装包中没有工作站登录服务器的参数和反病毒组件。

组安装包下载链接在用户组属性部分。

安装程序

代理端安装程序与安装包不同之处在于，安装程序不包含服务器连接参数和工作站登录服务器参数。

可以使用以下几种 Dr.Web代理端安装程序：

- OS Windows工作站有两种安装程序可用：
  - *网络安装程序*`drwinst.exe`可直接安装代理端。连接服务器后，代理端下载并安装必要反病毒软件包组件。使用网络安装程序可以本地方式和远程方式安装代理端。
    代理端网络安装程序`drwinst.exe`在Dr.Web服务器安装目录 `webmin/install`（默认情况下是隐藏的共享资源）。资源的网络访问在安装Dr.Web服务器时的步骤10指定。之后可自行更改这一资源。
  - *完整安装程序* `drweb-12.0.0-<编号>-esuite-agent-full-windows.exe`可同时安装代理端和反病毒软件包。
- OS Android、OS Linux、macOS工作站可使用Dr.Web代理端安装程序，与单机版安装程序类同。

Dr.Web代理端的安装程序可从Dr.Web安全管理中心的安装页面下载。



获取非OS Windows操作系统安装程序以及OS Windows安装程序完整版本，需安装Dr.Web服务器后从全球更新系统将**Dr.Web企业产品**加载到库。

使用服务器库的详细信息参见**管理员手册**中的Dr.Web服务器库的管理。

安装页面

从Dr.Web安全管理中心的安装页面可以下载：

1. Dr.Web代理端安装程序。

   Dr.Web Enterprise Security Suite支持的所有操作系统的受保护工作站安装程序与操作系统名称相对应的目录中。
2. 服务器证书`drwcsd-certificate.pem`。

可以从任意一台有Dr.We服务器访问权限的计算机登录安装页面，地址为：

`http://<服务器地址>:<端口号>/install`

其中 *<服务器地址>* 为安装有Dr.Web服务器的计算机的IP地址或域名。在 *<端口号>* 需输入端口号 9080(如果是https则为9081)。

5.2.2. 本地安装Dr.Web代理端

Dr.Web代理端本地安装直接在用户计算机或移动设备进行。管理员和用户皆可进行安装操作。



首次安装Dr.Web代理端 前需要更新服务器库(参见**管理员手册**中的 手动更新Dr.Web Enterprise Security Suite组件和检查**更新**)。

OS Android、OS Linux和macOS工作站

可使用下列方式在OS Android、OS Linux、macOS工作站进行Dr.Web代理端的本地安装:

- 个人安装包, 在管理中心创建。
- 管理中心创建的组安装包。
- Dr.Web代理端安装程序。

选择安装包类型时, 请注意:

a) 创建个人安装包时安装使用Dr.Web代理端安装程序, 以及连接服务器的参数和工作站登录服务器的参数。

b) 使用安装程序安装时安装Dr.Web代理端, 但没有连接服务器的参数和工作站登录服务器参数。

OS Windows工作站

可使用下列方式在OS Windows工作站进行Dr.Web代理端本地安装:

- 管理中心创建的个人安装包drweb_ess_*<OS>*_*<工作站>*.exe。
- 管理中心创建的组安装包drweb_ess_*<OS>*_*<组>*.exe。
- Dr.Web代理端完整安装程序drweb-12.0.0-*<编号>*-esuite-agent-full-windows.exe。
- Dr.Web代理端网络安装程序drwinst.exe。

选择安装包类型时, 请注意:

a) 从个人安装包进行安装时, 连接服务器的参数和工作站登录服务器参数包含在安装包内。从个人安装包安装基于网络安装程序安装, 只安装代理端, 连接到服务器后, 代理端下载并安装反病毒软件包组件。

b) 从组安装包安装时安装包中包含服务器连接参数以及安装代理端后工作站所属用户组的识别码和密码。但组安装包中没有工作站登录服务器的参数和反病毒组件。安装代理端后代理端会连接服务器。在时确定安装使用的组安装包所属用户组中是否存在可用工作站。存在可用工作站时工作站在服务器自动登录。

c) 网络安装程序仅安装代理端。连接到服务器后, 代理端下载并安装相应反病毒软件包组件。这种情况下不提供连接服务器的参数和工作站登录服务器参数。

d) 利用完整版本安装时同时安装代理端和反病毒软件包。不提供连接服务器的参数和工作站登录服务器参数。

对比安装文件

安装文件		代理端安装	安装反病毒软件包	服务器连接参数	服务器登录参数
安装包	个人安装包	+	–	+	+
	组安装包	+	–	+	–
安装程序	网络	+	–	–	–
	完整安装包	+	+	–	–

获取非OS Windows操作系统安装程序和安装包以及OS Windows安装程序完整版本，需安装Dr.Web服务器后从全球更新系统将**Dr.Web企业产品**加载到库。

使用服务器库的详细信息参见**管理员手册**中的Dr.Web服务器库的管理。

所有类型的代理端安装文件都可使用用户参数从命令行启动，参数列表见**附录**中的H1. 网络安装程序。

5.2.2.1. 利用个人安装包安装Dr.Web代理端

利用个人安装包将Dr.Web代理端安装到受保护工作站

1. 通过管理中心在Dr.Web 服务器为新用户创建账户。
2. 如用户自行安装Dr.Web代理端软件，需将相应操作系统过适用于移动设备的Dr.Web代理端组安装包链接发送给用户。

   为方便传输安装包和配置文件，可以使用**群发安装文件**功能（详细信息参见**管理员手册**中的群发安装文件），将相应文件发送至电子邮箱。

3. 在工作站安装Dr.Web代理端。

   工作站Dr.Web代理端本地安装介绍参见相应操作系统的**用户手册**。

   用户安装Dr.Web代理端应由具有该计算机管理员权限。

如果工作站已经安装反病毒软件，则安装开始前，安装程序会尝试将其删除。如果删除失败，则需要用户手动删除工作站上的反病毒软件。

4. macOS工作站连接Dr.Web服务器需在本地设置连接参数。

   使用个人安装包在其他支持的操作系统的工作站安装Dr.Web代理端时不需要进行补充设置。服务器连接参数和工作站登录服务器的参数包含于个人安装包。代理端安装后，工作站会自动连接服务器。

创建新工作站账户

创建新账户（一个或多个）需使用Dr.Web安全管理中心。

创建用户账户时注意管理中心以下页面指定的服务器名称：

1. **管理** → **服务器配置** → **Web服务器** → **Dr.Web服务器地址**一栏。该参数值在生成代理端安装包链接时给出。

   如果没有指定此参数值，则生成代理端安装程序下载链接将打开管理中心的计算机的DNS名称（如有）或其IP地址作为服务器名称。

2. **管理** → **Dr.Web服务器配置**→ 网络标签→ **加载**标签 → **Dr.Web服务器地址**一栏。该参数值写入代理端安装包，确定代理端连接的服务器。

   如果该参数值未给出，则创建代理端安装包时，在其中记录连接管理中心的服务器地址。此时，管理中心应根据创建账户的域IP地址连接服务器（服务器地址不应指定为loopback——127.0.0.1）。

通过Dr.Web安全管理中心创建新用户

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在工具面板点击按钮**添加网络对象**→ **创建工作站**。在管理中心窗口右侧将打开用户账户创建面板。
3. 在**数量**一栏输入需要创建的账户的数量。
4. 在识别码将自动生成所建工作站的独有识别码。如需可以更改这一识别码。
5. 在**名称**一栏指定工作站名称，这一名称将在反病毒网络分层楼板中显示。在工作站与服务器连接后这一名称可以自动更换为在本地设置的工作站名称。
6. 在**密码**和**确认密码**两栏输入工作站登录服务器的密码。如未指定密码，则自动生成。

   在创建一个以上账户时识别码、**名称**、**密码**（**确认密码**）各栏为自动给出，在创建工作站过程中无法进行更改。

7. 在**描述**一栏输入工作站补充信息。此栏可以不填写。
8. 在组部分选择新创建的工作站所归属的组。
   - 在**祖籍**一项可以设置工作站所属用户组列表。
     默认情况下工作站将列入**Everyone**组。如存在用户组，可选择工作站应归属的用户组，组数量不限。操作是在组**籍**部分列表勾选相应用户组。

不可将工作站从**Everyone**组和基组中删除。

为新建工作站指定基组的操作是在组**籍**部分点击相应组的图标。这时组图标上会出现**1**。

- 在**策略**可指定所建工作站继承设置的策略。
  默认不指定策略。指定是方式是勾选相应策略。工作站将从此策略当前版本继承设置。为一个工作站指定的策略不可超过一个。

9. 在**代理服务器**给出与此工作站连接的Dr.Web代理服务器的设置。
   如要在所建工作站安装代理服务器，需勾选此项创**建邻居代理服务器**并给出代理服务器参数。参数与创建代理服务器的参数相同。

创建工作站账户时管理中心将创建代理服务器账户。设置传送到工作站后在此工作站以背景模式安装代理服务器。代理端将只通过安装的代理服务器连接服务器。对用户而言，代理服务器为透明使用。

10. 必要时可填写**安全性**部分。此项设置详细描述见**管理**员**手册**中的安全性一节。
11. 必要时可填写**位置**一项。
12. 点击右上角的**保存**按钮。打开的窗口会显示新工作站已成功创建。这一窗口还显示代理端软件识别码和下列链接：
    - **安装文件**一项为代理端安装程序下载链接。
    - **配置文件**一项是OS Android、macOS和OS Linux下工作站连接Dr.Web服务器设置文件下载链接。

创建新工作站后和未指定工作站操作系统之前在软件下载部分分别列出Dr.Web Enterprise Security Suite支持的操作系统的相应链接。

代理端安装程序和配置文件下载链接还位于：

- 工作站创建后的属性部分。
- 在分层列表选择已创建的工作站后在**已**选择对**象**一项。

获取非OS Windows操作系统安装程序和安装包以及OS Windows安装程序完整版本，需安装Dr.Web服务器后从全球更新系统将**Dr.Web企**业产**品**加载到库。

使用服务器库的详细信息参见**管理**员**手册**中的Dr.Web服务器库的管理。

- 在**密**码一项输入此工作站登录服务器的密码。点击可显示密码。
- 在**代理服务器密**码一项输入代理服务器登录服务器的密码，如果创建工作站时有相关联的代理服务器(参见步骤9)。
- 在此窗口设有**安装**按钮，用于通过Dr.Web安全管理中心远程安装Dr.Web代理端。

13. 工作站Dr.Web代理端安装操作参见相关操作系统的**用**户**手册**。

macOS工作站连接Dr.Web服务器的连接设置

1. 在Dr.Web反病毒软件菜单点击设**置**并选择**模式**部分。

2. 勾选**启用统一保护模式**。
3. 配置文件`install.cfg`自动给出服务器连接设置，包括IP地址和服务器登录参数。配置文件含在个人安装包内。

   使用文件的操作：

   a) 在授权管理器打开**其他激活类型**链接。

   b) 在打开窗口拖动配置文件或点击虚线区域，打开文件选择窗口。

   连接文件后，服务器连接参数自动给出。

5.2.2.2. 利用组安装包安装Dr.Web代理端

利用组安装包将Dr.Web代理端安装到受保护工作站

1. 利用管理中心在Dr.Web服务器创建新的用户组（创建组操作详见**管理员手册**中的创建和删除组）。也可以使用之前创建的组。
2. 如需可在授权管理器为此组指定自身授权密钥。如不指定此组会从其父组继承授权密钥。
3. 利用管理中心在Dr.Web服务器为新工作站创建账户。将新的工作站账户列入第一步创建的用户组，并将此用户组指定为工作站的基组。可创建的工作站数量取决于此组可用授权的数量。
4. 组设置中将出现组安装包的链接。安装包按相应操作系统区分：一个安装包对应一个操作系统。
5. 如用户自行安装Dr.Web代理端软件，需将Dr.Web代理端组安装包链接发送给用户。向所有用户发送的是相应操作系统的同一个组安装包。
6. 在工作站安装Dr.Web代理端。



工作站Dr.Web代理端本地安装介绍参见相应操作系统的**用户手册**。



用户安装Dr.Web代理端应由具有该计算机管理员权限。

如果工作站已经安装反病毒软件，则安装开始前，安装程序会尝试将其删除。如果删除失败，则需要用户手动删除工作站上的反病毒软件。

7. 安装代理端后代理端会连接组安装包中指定的服务器。在第一次连接服务器时确定代理端安装使用的组安装包所属用户组中是否存在可用工作站。可用工作站数量取决于未到期的可用账户数量。每一次组安装包连接后重新计算可用工作站数量。

   a) 存在可用工作站时工作站在服务器自动登录。此过程不需要管理员参与。

   b) 没有可用工作站时，中断安装并向用户显示相应通知。

5.2.2.3. 利用安装程序安装Dr.Web代理端

代理端安装程序与安装包不同之处在于，安装程序不包含服务器连接参数和工作站登录服务器参数。

Dr.Web代理端的安装程序可从Dr.Web安全管理中心的安装页面下载。

获取非OS Windows操作系统安装程序以及OS Windows安装程序完整版本，需安装Dr.Web服务器后从全球更新系统将**Dr.Web企业产品**加载到库。

使用服务器库的详细信息参见**管理员手册**中的Dr.Web服务器库的管理。

在OS Android、OS Linux、macOS工作站进行本地安装

OS Android、OS Linux、macOS工作站可使用Dr.Web代理端安装程序，与单机版安装程序类同。

工作站Dr.Web代理端本地安装介绍参见相应操作系统的**用户手册**。

如果通过没有配置文件的安装程序进行安装，则需要在工作站手动输入工作站要连接的服务器地址。

可以手动指定登录参数或不指定。可使用下列方式连接服务器：

任务选项	登录参数
手动指定	尝试根据指定登录参数自动登录。
不指定	登录服务器的方式取决于新工作站连接的服务器的设置（详情参见**管理员手册**中的 工作站连接策略）。

手动设置登录参数，必须首先在管理中心创建新工作站帐户。将可访问包含连接和登录参数配置文件的安装包。建议使用安装包代替安装程序。

Windows操作系统工作站的本地安装

可以使用以下几种 Dr.Web代理端安装程序：

- *网络安装程序* `drwinst.exe`仅用于安装代理端。连接服务器后，代理端下载并安装相应的反病毒软件包组件。
- *完整安装程序* `drweb-12.0.0-<编号>-esuite-agent-full-windows.exe`可同时安装代理端和反病毒软件包。

利用这些安装程序安装时可不指定连接服务器的参数和登录参数或手动指定这些参数。

手动设置登录参数，必须首先在管理中心创建新工作站帐户。将可访问包含连接登录参数配置文件的安装包。如果无需使用完整版本或网络安装程序进行安装，建议使用安装包代替安装程序。

可用下列方式连接服务器：

任务选项	服务器地址	登录参数
手动指定	工作站直接连接指定的服务器。	尝试根据指定登录参数自动登录。
不指定	代理端利用*服务器搜索服务*在网络搜索服务器。尝试连接搜索到的第一个服务器。	登录服务器的方式取决于新工作站连接的服务器的设置（详情参见**管理员手册**中的 工作站连接策略）。

如何使用完整安装程序和安装包安装Dr.Web代理端参见OS Windows用户手册。

利用网络安装程序进行安装建议由反病毒网络管理员来完成。

使用Windows操作系统网络安装程序进行本地安装

代理端网络安装程序drwinst.exe仅用于安装Windows操作系统代理端。

如果在已完成安装的工作站上网络安装程序是以正常安装模式启动（即没有使用参数/instMode remove），则不会执行任何操作。安装程序结束运行后会显示可用参数窗口。

使用网络安装程序进行安装可以选用两种模式：

1. *背景模式*——如果指定的是背景模式相应参数，则启动此模式。
2. *图形模式*——默认模式。如果未指定背景模式参数，则启动此模式。

还可使用网络安装程序将Dr.Web 代理端远程安装到工作站，远程安装可以通过管理中心（参见 Dr.Web代理端远程安装）。

以安装程序背景模式在工作站上安装Dr.Web代理端

1. 从需要安装反病毒软件的计算机进入代理端网络安装目录（在安装服务器时这是服务器安装目录子目录webmin/install，之后可将此目录转移）或从管理中心 安装页面下载安装程序执行文件drwinst.exe和证书drwcsd-certificate.pem。使用背景模式参数/silent yes启动文件drwinst.exe。

   默认下没有服务器连接参数的文件drwinst.exe使用*Multicast*模式扫描网络，搜索处于活动状态的Dr.Web服务器，并尝试从在网络中找到的第一个服务器进行代理端安装。

   使用*Multicast*模式搜索处于活动状态的服务器时，会从找到的第一个服务器进行代理端安装。这时如果现有的加密公钥与服务器密钥不符，安装过程会出现错误。在这种情况下在启动安装程序时需明确指定服务器地址（见下）。

   如果需要在安装服务器的计算机安装代理端，需直接在安装程序启动参数中指定服务器地址，因为通过multicast搜索时可能发现不了服务器。

   可以添加不同参数运行文件drwinst.exe：

   - 如不使用*Multicast*模式，安装代理端时建议使用服务器名称（事先已在DNS服务中注册的名称）：

```
drwinst /silent yes /server <服务器DNS名称>
```

这样做如果将来Dr.Web服务器安装到另一台计算机，可以简化反病毒网络设置过程。

- 也可以直接指明服务器地址，例如：

```
drwinst /silent yes /server 192.168.1.3
```

- 使用参数/regagent yes可在安装时在添加和删除的程序列表中注册代理端。

网络安装程序所有参数列表见附录中的H1. 网络安装程序。

2. 安装程序运行结束后计算机上将安装反病毒代理端软件（而非反病毒软件包）。
3. 工作站在服务器上得到确认后（如果服务器的设置为要求确认工作站）将自动安装反病毒软件包。
4. 按照代理端要求重新启动计算机。

以安装程序图形模式将Dr.Web代理端安装到工作站的操作

从需要安装反病毒软件的计算机进入代理端网络安装目录（在安装服务器时这是服务器安装目录子目录webmin/install，之后可将此目录转移）或从管理中心 安装页面下载安装程序执行文件drwinst.exe和证书drwcsd-certificate.pem。启动文件drwinst.exe。

打开Dr.Web代理端安装向导窗口。使用网络安装程序图形模式安装代理端的以下步骤与使用安装包安装相同，但不设置与服务器的连接，如果命令行相应参数中未作连接设置。

工作站代理端的安装参见**Windows操作系统Dr.Web代理端。用户手册**。

5.2.3. OS Windows下Dr.Web代理端的远程安装

Dr.Web Enterprise Security Suite可以识别出还没有安装Dr.Web Enterprise Security Suite反病毒保护的计算机，并且在一些情况下可以进行反病毒保护的远程安装。

可以通过以下方式进行远程安装：

- 利用管理中心。
- 如果受保护的局域网中使用Active Directory，则通过此项服务安装。

Dr.Web代理端只能远程安装到Windows操作系统的工作站（参见附录中的 附录A. 产品支持的所有操作系统列表），但不包括Starter和Home版本。

将Dr.Web代理端远程安装到工作站需要具备这些工作站的管理员权限。

如果远程工作站在域中并使用域管理员账户，通过管理中心进行远程安装时需要在工作站启用文件和打印机共享（Windows操作系统不同版本下此设置所在位置见下表）。

如果网络工作站不在域中，或使用本地账户安装，则部分 Windows版本要求对工作站进行补充设置。

远程安装时对域外工作站或使用本地账户的工作站进行补充设置

这些设置有可能会降低网络计算机的安全等级。请在对系统做出更改前了解这些设置的用途，或者放弃远程安装，选择手动安装代理端。

设置网络工作站之后，建议将所有自定义设置恢复到编辑之前的设置值，以免破坏操作系统安全的基本策略。

对不在域中和/或使用本地账户工作站进行代理端远程安装，需要在将安装代理端的工作站完成以下操作：

操作系统	设置	
Windows XP	设置对共享文件的访问模式	新视窗： **开始**→设置→**控制面板** → **外观和主题** → **文件夹属性**→ 查看 标签 → 取消对**使用**简单**文件共享（推荐）**一项的勾选
		经典视窗： **开始**→设置→**控制面板** → **文件夹属性**→ 查看 标签 → 取消对**使用**简单**文件共享（推荐）**一项的勾选
	在本地安全策略中将网络身份验证设置为：	新视窗： **开始**→设置→**控制面板** → **性能和维护** → **管理工具** → **本地安全策略** → **安全设置** → **本地策略** → **安全选项** → **网络访问：本地账户的共享和安全模式** → 经典——**本地用户以自己的身份**验证。
		经典视窗： **开始**→ 设置→**控制面板** → **管理工具** → **本地安全策略** → **安全设置** → **本地策略** → **安全选项** → **网络访问：本地账户的共享和安全模式** → 经典——**本地用户以自己的身份**验证。
	远程安装前在工作站禁用Windows Firewall。	
Windows Server 2003	远程安装前在工作站禁用Windows Firewall。	
Windows Vista Windows Server 2008	开启文件共享	新视窗： **开始**→设置→**控制面板** → **网络和Internet** → **网络和共享中心** → **共享和发现** → **文件共享** → **启用**。
		经典视窗：

<table>
<tr><th>操作系统</th><th colspan="2">设置</th></tr>
<tr><td rowspan="4"></td><td></td><td>开始→设置→控制面板 → 网络和共享中心 → 共享和发现 → 文件共享 → 启用。</td></tr>
<tr><td rowspan="2">在本地安全策略中将网络身份验证设置为:</td><td>新视窗:

开始→设置→控制面板 → 系统和维护 → 管理工具 → 本地安全策略 → 安全设置 → 本地策略 → 安全选项 → 网络访问:本地账户的共享和安全模式 → 经典——本地用户以自己的身份验证。</td></tr>
<tr><td>经典视窗:

开始→控制面板 → 管理工具 → 本地安全策略 → 安全设置 → 本地策略 → 安全选项 → 网络访问:本地账户的共享和安全模式 → 经典 - 本地用户以自己的身份验证。</td></tr>
<tr><td colspan="2">创建密钥LocalAccountTokenFilterPolicy:

a) 在注册表编辑器中打开分支 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System。如果不存在记录 LocalAccountTokenFilterPolicy, 在修改菜单选择创建并指定DWORD。输入LocalAccountTokenFilterPolicy并点击ENTER。
b) 在选项LocalAccountTokenFilterPolicy菜单选择更改。
c) 在数值一栏指定数值 1并点击确定。

无需重启。</td></tr>
<tr><td rowspan="4">Windows 7

Windows Server 2008 R2</td><td rowspan="2">启用文件和打印机共享</td><td>新视窗:

开始→控制面板 → 网络和Internet → 网络和共享中心 → 更改共享补充参数 → 文件和打印机共享 → 启用文件和打印机共享。</td></tr>
<tr><td>经典视窗:

开始→控制面板 → 网络和共享中心 → 更改共享补充参数 → 文件和打印机共享 → 启用文件和打印机共享。</td></tr>
<tr><td rowspan="2">在本地安全策略中将网络身份验证设置为:</td><td>新视窗:

开始→控制面板 → 安全系统 → 管理工具 → 本地安全策略 → 安全设置 → 本地策略 → 安全选项 → 网络访问:本地账户的共享和安全模式 → 经典 - 本地用户以自己的身份验证。</td></tr>
<tr><td>经典视窗:

开始→控制面板 → 管理工具 → 本地安全策略 → 安全设置 → 本地策略 → 安全选项 → 网络访问:本地账户的共享和安全模式 → 经典 - 本地用户以自己的身份验证。</td></tr>
<tr><td colspan="2">创建密钥LocalAccountTokenFilterPolicy:

a) 在注册表编辑器中打开分支 HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion</td></tr>
</table>

操作系统	设置	
	\Policies\System。如果不存在记录 **LocalAccountTokenFilterPolicy**，在**修改**菜单选择**创建并指定DWORD**。输入**LocalAccountTokenFilterPolicy**并点击ENTER。 b) 在选项**LocalAccountTokenFilterPolicy**菜单选择**更改**。 c) 在**数值**一栏指定数值 **1**并点击**确定**。 无需重启。	
Windows 8 Windows 8.1 Windows Server 2012 Windows Server 2012 R2 Windows 10	启用文件和打印机共享	新视窗： 选项 → **控制面板** → 网络和**Internet** → 网络和共享中心 → **更改共享补充参数** → **文件和打印机共享** → **启用文件和打印机共享**。
		经典视窗： 选项 →**控制面板** → **网络和共享中心** → **修改共享补充参数** → **文件和打印机共享** → **启用文件和打印机共享**。
	在本地安全策略中将网络身份验证设置为：	新视窗： 选项 →**控制面板** → **安全系统** → **管理工具** → **本地安全策略** → **安全设置** → **本地策略** → **安全选项** → **网络访问：本地账户的共享和安全模式** → **经典 - 本地用户以自己的身份验证**。
		经典视窗： 选项 →**控制面板** → **管理工具** → **本地安全策略** → **安全设置** → **本地策略** → **安全选项** → **网络访问：本地账户的共享和安全模式** → **经典 - 本地用户以自己的身份验证**。
	创建密钥**LocalAccountTokenFilterPolicy**： a) 在注册表编辑器中打开分支 **HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System**。如果不存在记录 **LocalAccountTokenFilterPolicy**，在**修改**菜单选择**创建并指定DWORD**。输入**LocalAccountTokenFilterPolicy**并点击ENTER。 b) 在选项**LocalAccountTokenFilterPolicy**菜单选择**更改**。 c) 在**数值**一栏指定数值 **1**并点击**确定**。 无需重启。	

如果网络中工作站上账户密码为空，需要在本地安全策略中设置使用空白密码进行访问：**控制面板** → **管理工具** → **本地安全策略** → **安全设置** → **本地策略** → **安全选项** → 账户：**使用空白密码的本地账户只允许进行控制台登录** → **已禁用**。

5.2.3.1. 通过Dr.Web安全管理中心安装Dr.Web代理端

可以通过以下方式将代理端远程安装到网络中的工作站：

1. 利用网络搜索仪进行安装。

   可先搜索网络中未受保护的计算机，然后进行Dr.Web代理端的安装。

2. 利用网络安装工具进行安装。

   如预先知道需安装代理端的工作站或工作站组的地址，可以使用这一方式进行安装。

3. 以指定ID 安装到工作站。

   指定访问服务器的ID和密码，在所账户下（包括在所现新账户下）将代理端安装到工作站和工作站组。



Windows Internet Explorer浏览器下网络搜索仪和网络**安装**工具正常运行需要将安装有Dr.Web服务器的电脑的IP地址和/或DNS名称添加到打开管理中心的浏览器可信任网址。

使用网络搜索仪

管理中心反病毒网络分层列表中显示的是已加入反病毒网络的计算机。Dr.Web Enterprise Security Suite 还具备发现尚未安装Dr.Web Enterprise Security Suite反病毒软件包保护的计算机并进行反病毒组件的远程安装的功能。

建议使用网络搜索仪（参见**管理**员**手册**中的网络搜索仪）对计算机进行IP地址搜索，以便将代理端软件迅速安装到工作站。

使用网络搜索仪安装Dr.Web代理端

1. 打开网络搜索仪。打开操作是在管理中心主菜单中选择**管理**一项，在打开的窗口选择网络**搜索**仪，即打开同名窗口。
2. 对搜索参数进行设置。设置的详细介绍见**管理**员**手册**中的网络搜索仪。
3. 点击扫**描**按钮。在此窗口将加载计算机目录（分层列表），标志有哪些计算机已安装有反病毒软件，哪些没有安装。
4. 展开目录各项，每项各对应工作站组（域）。各项均注有图标，各图标含义见下表。

   表 5-1. 可能显示的图标

图标	**描述**
工作站组	
	组中有的计算机可以安装Dr.Web Enterprise Security Suite反病毒软件。
	组中工作站已安装有反病毒软件或者工作站无法从网络访问。
工作站	
	工作站已安装有反病毒软件，处于活跃状态。
	工作站处于活跃状态，反病毒软件状态不确定：工作站未安装反病毒软件，或未检查是否安装有反病毒软件。

   对应标志有的工作站的目录项可继续展开，查看已安装的组件。

5. 在网络**搜索**仪窗口选择未受保护的计算或多台未受保护的计算机（利用CTRL或SHIFT键）。
6. 在工具面板点击**安装Dr.Web代理端**按钮。
7. 打开网络**安装**窗口，指定代理端安装任务。

8. 在**工作站地址**给出要安装Dr.Web代理端的工作站的IP地址或DNS名称。多个工作组时使用"；" 或"，" 作为隔开符（隔开符前后的空格无效）。

   向通过网络搜索仪找到的工作站进行安装时，在**工作站地址**一栏会给出将进行安装的一台或多台工作站的地址。

   地址以网络格式输入，网络格式列于**附**录中的附录E. 网络地址特点。

9. 默认情况下代理端软件将安装到工作站文件夹`%ProgramFiles%\DrWeb`。如需可在**Dr.Web代理端安装目**录一栏指定另一路径。

   建议指定完整路径以便准确确定安装目录位置。指定路径时允许使用环境变量。

10. 默认情况下**Dr.Web服务器**一栏显示管理中心连接的Dr.Web服务器的IP地址或DNS名称。如需可在此栏指定将从其进行反病毒软件安装的服务器的地址。指定多个服务器时，需使用"；"或"，" 作为分隔符（隔开符前后的空格无效）。如为空，则使用Dr.Web服务器发现服务（*Multicast*模式）。

    无法对安装有启动安装进程的服务器的计算机进行代理端的远程安装。

    地址以网络格式输入，网络格式列于**附**录中的附录E. 网络地址特点。

11. 在语**言**下拉列表中选择安装在工作站上的Dr.Web反病毒软件界面语言。
12. 在**同时安装数量**一栏指定可以进行远程安装的最多工作站数量。
13. 在**安装超**时时**限（秒）**一栏指定完成代理端安装的最长时限（以秒计）。允许值为：1-600。默认值为180秒。如服务器与代理端间带宽有限，建议将此值增大。
14. 如需，可勾选**在已安装程序列表中注册Dr.Web代理端**。
15. 在**可安装组件**部分选择需要安装到工作站的反病毒软件包组件。
16. 在压缩和**加密**部分指定网络安装程序安装代理端和反病毒软件包时流量压缩和加密参数。安装后代理端使用这些参数与服务器交互作用。
17. 在**登**录远**程工作站**部分给出访问将安装代理端的远程计算机的登录参数：
    - **用**户——登录进行远程安装的工作站所使用的用户名。域用户需使用域名格式 *<域>*\ *<用户>*或 *<用户>*@ *<域>*。本地用户需使用工作站名称或工作站组名称，格式为 *<工作站>*\ *<用户>*或 *<组>*\ *<用户>*。
    - **密**码——远程计算机的用户密码。

    可以同时设定几个管理员账户。再添加一个账户栏需再次点击按钮 + 后重新填写登录设置。添加每一新账户操作相同。

    安装代理端时首先使用列表中的第一个账户。如使用第一个账户未能成功安装，则依次使用下一个账户。
18. 在输入所有必要参数后点击**安装**。

    启动反病毒软件包安装使用内置服务软件。

启动安装使用的是位于服务器安装目录的webmin\install\windows中的当前服务器网络安装程序，以及位于服务器安装目录的etc中的SSL证书drwcsd-certificate.pem。

19. Dr.Web代理端将安装到指定的工作站。工作站在服务器上获得确认后（如果Dr.Web 服务器设置为要求确认，参见**管理员手册**中的工作站连接策略），将自动安装反病毒软件包。
20. 按照代理端要求重新启动计算机。

使用网络安装工具

如反病毒网络已基本建成后需要将代理端软件安装到一些计算机，建议使用**网络安装**。

通过网络安装Dr.Web代理端

1. 选择主菜单中的**管理**一项。在打开的窗口选择**网络安装**。
2. 以下步骤同上的**8-21**。

以指定ID 为一定账户进行安装

创建工作站新账户时：

1. 创建一个或几个工作站新账户（参见创建新账户一节）。
2. 创建新账户后在主窗口右侧即会打开标题为**创建工作站**的面板。点击**安装**按钮。
3. 打开网络搜索仪窗口。
4. 以下步骤同上的**2-21**。
5. 安装结束后请检查分层列表，相应工作站的图标会发生改变。

使用工作站现有账户时：

1. 在反病毒网络分层列表中择未安装代理端的新工作站、工作站组，或择**New**组（为所有新账户进行安装）。
2. 在工具面板点击**安装Dr.Web代理端**按钮。
3. 打开网络搜索仪窗口。
4. 以下步骤同上的**2-21**。
5. 安装结束后请检查分层列表，相应工作站的图标会发生改变。

组管理员也可以指定ID将代理端安装到工作站。

远程安装出错时请参阅**附录** 远程安装错误诊断。

5.2.3.2. 通过Active Directory服务安装代理端

如果受保护的局域网中使用**Active Directory**，可以将Dr.Web代理端远程安装到工作站。

通过Active Directory安装代理端还可以利用分布式文件系统DFS（参见**附**录中的使用DFS通过Active Directory安装代理端）。

代理端安装

通过Active Directory服务安装代理端的操作

1. 选择主菜单的**管理**一项，之后在控制菜单选择库**常规配置**。
2. 打开标签**Dr.Web安装包** → **Dr.Web企业产品**.
3. 勾选**用于Active Directory的Dr.Web代理端**。点击**保存**。
4. 利用控制菜单的库**状态**部分更新库。
5. 从GUS加载后安装页面会出现用于带有**Active Directory**的网络的Dr.Web代理端安装程序的链接：

   `https://<服务器地址>:<端口号>/install/activedirectory`

   其中*<服务器地址>*为安装有Dr.Web服务器的计算机的IP地址或域名。在*<端口号>*需输入端口号`9080`（如果是http则为`9081`）。
6. 从安装页面加载用于带有**Active Directory**的网络的Dr.Web代理端安装程序。
7. 在支持**Active Directory**服务的局域网服务器完成Dr.Web代理端高级安装。安装可使用命令行模式**(A)**，也可以使用安装程序的图形模式**(B)**。

更新服务器时不需要一定更新用于带有Active Directory的网络的Dr.Web代理端安装程序。服务器软件更新结束后，工作站上的代理端和反病毒软件会在安装后自动更新。

(A) 命令行模式下Dr.Web代理端安装参数的设置

启动以下命令行，使用所有必要参数和关闭图形模式的参数`/qn`：

`msiexec /a <软件包名称>.msi /qn [<参数>]`

参数`/a`是用于启动部署管理员软件包。

软件包名称

用于带有**Active Directory**的网络的Dr.Web代理端安装包的名称一般使用以下格式：

`drweb-12.00.0-<编号>-esuite-agent-activedirectory.msi`

参数

`/qn`——是关闭图形模式的参数。使用这一参数时必须指定以下强制参数：

- ESSERVERADDRESS=*<DNS名称>*——代理端将连接的Dr.Web服务器的地址。可使用的格式参见附录中的附录E。
- ESSERVERPATH=*<文件网站名称>*——指定Dr.Web服务器加密公钥的完整路径和文件名称(默认情况下文件drwcsd.pub在Dr.Web服务器安装目录的子目录webmin/install)。
- TARGETDIR——代理端样式(已修改的代理端安装包)的网络目录，该目录通过所指定安装的组策略编辑器选择。对此目录应可进行读取和写入访问。目录即便是可从本地访问，其路径也应以网络地址格式给出；目录要一定能够从目标工作站进行访问。



高级安装前不需要手动将安装文件移至代理端镜像(参见参数TARGETDIR)的目标文件夹。用于有Active Directory的网络的代理端安装程序(*<软件包名称>*.msi)以及在工作站安装代理端所需的其他文件将在高级安装过程中自动进入目标文件夹。如果开始高级安装前目标文件夹中已有此类文件，如上次安装使用的文件，则同名文件将被覆盖。

如需要从不同服务器进行高级安装，建议给每个服务器设置不同的目标目录。



部署管理员软件包后在目录*<目标文件夹>*\Program Files\DrWeb 应只有README.txt一个文件。

示例

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=servername.net ESSERVERPATH=\
\win_serv\drwcs_inst\drwcsd-certificate.pem TARGETDIR=\\comp\share
```

```
msiexec /a ES_Agent.msi /qn ESSERVERADDRESS=192.168.14.1 ESSERVERPATH="C:
\Program Files\DrWeb Server\webmin\install\drwcsd-certificate.pem"
TARGETDIR=\\comp\share
```

在安装程序图形模式中也可指定上述参数。

之后必须在安装有Active Directory管理软件的局域网服务器上设定安装软件包(见下)。

(B) 图形模式下Dr.Web代理端安装参数的设置



高级安装前请确认代理端镜像的目标文件夹中不应有用于带有**Active Directory**的网络的Dr.Web代理端安装程序(*<软件包名称>*.msi)。



部署管理员软件包后在目录*<目标文件夹>*\Program Files\DrWeb应只有README.txt一个文件。

1. 在图形模式下启动安装程序需执行以下命令：

```
msiexec /a <安装程序路径>\<软件包名称>.msi
```

2. 打开**InstallShield Wizard**窗口，窗口显示要安装的产品信息。点击**下一步**。

代理端安装使用的语言是计算机语言设置中指定的语言。

3. 在新窗口中输入Dr.Web服务器的DNS名称或IP地址(参见**附录**中的附录E)。给出Dr.Web服务器证书(drwcsd-certificate.pem)**所在位置**。**点击下一步**。
4. 在下一个窗口中指定将写入代理端镜像的网络目录。该目录即便是可从本地访问，其路径也应以网络地址格式给出；该目录要一定能从目标工作站进行访问。**点击安装**。
5. 安装结束后将自动显示设置窗口，利用设置窗口可以设定将软件包安装到计算机网络。

工作站软件包安装设置

1. 在**控制面板**(或是Windows 2003/2008/2012/2012R2 Server操作系统下**开始菜单**、Windows 2000 Server操作系统下**开始菜单** → **所有程序**)选择**管理工具** → **Active Directory ——用户和计算机**(代理端安装图形模式下会自动显示此设置窗口)。
2. 在将进行Dr.Web代理端安装的计算机所在域建立一个新的**单位**(在Windows 2000 Server操作系统下是组织**单位**)，单位名称可以是**ESS**。建立单位需在域上下文菜单中选择**创建** → **单位**。在打开的窗口输入新单位的名称后点击**确定**。把需要安装代理端的计算机纳入新创建的单位。
3. 打开组策略编辑窗口。操作是：
   a) Windows 2000/2003 Server操作系统下：在新创建单位**ESS**的菜单中选择**属性**。在打开的属性窗口进入组**策略**标签。
   b) Windows 2008/2012/2012R2 Server操作系统下：**开始** → **管理工具** → 组**策略管理**。
4. 为新创建的单位设置组策略。操作是：
   a) Windows 2000/2003 Server操作系统下：**点击添加**按钮，建立策略名称为**ESS**的列表项，然后双击此项。
   b) Windows 2008/2012/2012R2 Serv操作系统下：在新创建单位 **ESS**的上下文菜单中选择**在这个域中创建GPO并在此处链接**。在打开的窗口为组策略新对象指定名称，然后点击**确定**。在新组策略上下文菜单中选择**更改**。
5. 在打开的组**策略编辑器**窗口输入在第**4**步建立的组策略的设置。操作是：
   a) Windows 2000/2003 Server操作系统下：在分层列表中选择计**算机配置** → **软件配置** → **软件安装**。
   b) Windows 2008/2012/2012R2 Server操作系统下：在分层列表中选择计**算机配置** → **策略** → **软件配置** → **软件安装**。
6. 在**软件安装**菜单中选择**创建** → **软件包**。
7. 接下来指定代理端安装包，需给出网络共享资源地址(高级安装时建立的代理端样本)。该文件夹即便是可从本地访问，其路径也应以网络地址格式给出。
8. 打开**部署软件**对话框中选择**已发布**选项后，**点击确定**按钮。
9. 在组策略编辑器窗口会出现**Dr.Web Agent**。在此项的菜单中选择**属性**。
10. 在打开的软件包属性窗口进入**部署**标签，**点击高级**按钮。
11. 打开**部署高级设置**窗口。
    - 勾选**部署不使用语言设置**。
    - 如果要使用自定义msi安装包将Dr.Web代理端安装到64位操作系统，请勾选**将此32位应用程序转为可用于x64机**。
12. 连续**两次点击确定**按钮。

13.Dr.Web代理端将在所选计算机在域中最近一次注册时安装到计算机上。

曾安装过代理端时的策略应用

为代理端安装指定Active Directory策略时必须考虑工作站上是否安装有代理端。可能会有三种情况：

1. **工作站上没有Dr.Web代理端。**

   应用策略后代理端将按照共同规则安装。

2. **工作站上已安装有Dr.Web 代理端，安装时没有使用Active Directory服务。**

   应用Active Directory策略后工作站上将保留已安装的代理端。

   在这种情况下代理端已安装在工作站，但Active Directory会认为代理端还没有安装，因此工作站每次启动时Active Directory都会重复安装代理端的失败尝试。

   通过Active Directory安装代理端时必须手动（或利用管理中心）删除先前安装的代理端，然后再次为该工作站指定Active Directory策略。

3. **工作站上已安装有Dr.Web 代理端，安装使用的是Active Directory服务。**

   如工作站Dr.Web代理端安装使用的是Active Directory服务，不需再次指定策略。

   指定应用策略不会使工作站上反病毒软件的状态发生变化。

5.3. NAP Validator的安装

Dr.Web NAP Validator 的用途是检查受保护工作站上反病毒软件的工作性能。

该组件安装于设有NAP服务器的计算机。

安装NAP Validator

1. 启动程序文件。打开语言选择窗口，产品以下安装将使用在这一窗口所选择的语言。请选择所需要的语言，然后点击**下一步**。
2. 打开**InstallShield Wizard**窗口，窗口显示要安装的产品信息。点击**下一步**。
3. 打开及许可协议窗口。了解许可协议条款后需选择**我接受许可协议的条款**并点击**下一步**按钮。
4. 在打开窗口的**地址**和**端口**两栏分别给出Dr.Web服务器的IP地址和端口，然后点击**下一步**。
5. 点击**安装**按钮。接下来的安装过程不再需要用户的参与。
6. 安装结束后请点击**完成**。

Dr.Web NAP Validator安装完成后必须将Dr.Web服务器列入NAP可信任服务器组。操作是：

1. 打开NAP服务器设置组件（命令为`nps.msc`）。
2. 在**修复服务器组**部分点击**添加**按钮。
3. 在打开的对话窗口给出修复服务器名称和Dr.Web服务器的IP地址。
4. 点击**确定**按钮保存修改。

5.4. Dr.Web代理服务器的安装

反病毒网络可以包括一个或几个代理服务器。

选择在哪台计算机安装代理服务器时，主要的标准是从由代理服务器中转信息的所有网络/网段都能够访问这台计算机。

可用以下一个方式在OS Windows安装代理服务器：

- 在安装Windows操作系统Dr.Web代理端的过程中进行自动安装

  安装使用Dr.Web代理端个人安装包，创建个人安装包时指定了安装邻居代理服务器的设置。这时以背景模式自动安装代理服务器。
- 在已安装有Windows操作系统Dr.Web代理端的工作站自动安装

  在管理中心指定安装邻居代理服务器的设置。将以背景模式自动安装代理服务器。
- 使用安装程序图形界面手动安装

  管理员选择网络中任意一台适合的工作站手动安装。此工作站可不安装任何其他反病毒网络组件。

在UNIX家族操作系统安装代理服务器只能利用安装程序手动安装。

5.4.1. 创建Dr.Web代理服务器账户



管理员需在代理服务器将连接的每一台服务器（流量转输到的服务器）创建代理服务器账户。

通过Dr.Web安全管理中心创建代理服务器账户

1. 在要创建代理服务器的父组按照**管理员手册**远程设置代理服务器指定设置。这时代理服务器连接时会继承指定的设置。也可在创建代理服务器账户后指定设置（可通过父组继承，也可指定自身设置），但必须在代理服务器连接所创建的账户之前进行设置。

   如未在代理服务器连接所创建的账户之前进行设置，则不会加载配置文件。代理服务器将使用当前设置，直至其所连接的服务器指定新的设置，前提是该服务器允许对配置进行管理。
2. 在管理中心主菜单选择**反病毒网络**一项。
3. 创建代理服务器的操作取决于是在已有Dr.Web代理端的工作站进行安装，还是单独安装代理服务器：

№	操作	同代理端一起安装	单独安装
a)	1. 在反病毒网络树结构选择要安装邻居代理服务器的工作站。 2. 在所选工作站属性面板进入**代理服务器**部分。	+	–
b)	1. 在反病毒网络树结构选择要安装邻居代理服务器的工作站。 2. 在工具面板选择**添加网络对象**→**创建代理服务器**。	+	+

№	操作	同代理端一起安装	单独安装
c)	1. 确认在反病毒网络树结构没有选择如何工作站。 2. 在工具面板选择**添加网络对象**→**创建代理服务器**。	+	+

如果创建代理服务器账户后在已有代理端的工作站安装，则创建代理服务器账户后代理端会以背景模式自动安装代理服务器（另见在安装Windows操作系统Dr.Web代理端的过程中安装Dr.Web代理服务器）。

如果创建代理服务器账户后进行单独安装（不通过代理端），则需管理员利用与服务器软件包一同提供的安装包手动安装代理服务器。

4. 在**识别码**一栏将自动生成所建账户的独有识别码。如需可以更改这一识别码。
5. 在**名称**一栏指定在反病毒网络树结构显示的代理服务器名称。

设置时给出的名称在代理服务器连接到服务器后会自动更换为计算机名称。

6. 在**密码**和**确认密码**两栏输入代理服务器登录服务器的密码。如未指定密码，则自动生成。

代理服务器密码和识别码固定。需在代理服务器连接的所有服务器创建识别信息相同的代理服务器账户（见Dr.Web代理服务器连接Dr.Web服务器）。

创建代理服务器账户后无法编辑识别码。

7. 3.b)和3.c)两步**工作站**一栏给出安装有代理端的现有工作站，此代理服务器与之相邻。

   3.b)一步**工作站**一栏将自动给出所选工作站的识别码。

   3.c)一步**工作站**一栏将为空。

   - 指定安装代理服务器的工作站的操作是点击后在打开的窗口选择反病毒网络树结构中的一个现有工作站。
   - 让**工作站**一栏为空，以便代理服务器不与任何工作站为邻且连接手动安装的代理服务器。如**工作站**不为空，需点击删除。
8. 在**组籍**指定所建代理服务器归属的组。更改方式是勾选列表中所需组。

   每一代理服务器只能列入一个组。

   可选择组**Proxies**或其子组。
9. 点击**保存**按钮。

   打开代理服务器账户已成功创建的窗口，此窗口包含访问服务器的密码。显示密码需点击。

管理员将代理服务器连接服务器时需要使用通过管理中心创建的代理服务器账户的识别码和密码：

- 利用图形安装程序在代理服务器安装过程中建立连接。
- 安装代理服务器后建立连接（仅限UNIX家族操作系统）。

5.4.2. 在安装Windows操作系统Dr.Web代理端的过程中安装Dr.Web代理服务器

与Windows操作系统Dr.Web代理端一起安装Dr.Web代理服务器

1. 在管理中心按照**管理员手册**远程设置代理服务器指定设置。应为要创建代理服务器的父组指定设置。这时创建时会继承指定的设置。也可在创建代理服务器账户后指定设置(可通过父组继承，也可指定自身设置)，但必须在代理服务器连接所创建的账户之前进行设置。

   如未在代理服务器连接前指定，将使用安装器发给代理服务器的设置。这些设置意味着只与安装代理服务器的服务器建立连接。

2. 按照利用个人安装包安装Dr.Web代理端的描述通过管理中心创建工作站账户。在创建工作站过程中勾选**创建邻居代理服务器**并给出相应设置，包括代理服务器所应归属的组，在步骤1已为此组指定了设置。

   只有创建账户时可以更改代理服务器的识别码。

3. 在工作中启动从步骤2创建的个人安装包安装代理端。
4. 代理端安装后自动从服务器加载代理服务器安装器，并在此工作站以背景模式启动。服务器证书和地址以及连接服务器所选的识别信息会自动写入代理服务器的相应配置文件。代理服务器设置中指定只将流量定向到安装代理服务器的服务器。
5. 安装后代理服务器连接实施安装的服务器获取完整的配置文件。如进行步骤1时没有在服务器给出设置，则不会加载配置文件。将使用安装器给出的设置，直至所连接的服务器给出新设置。
6. 代理端将只通过安装的代理服务器连接服务器。对用户而言，代理服务器为透明使用。

5.4.3. 利用安装程序安装Dr.Web代理服务器

代理服务器的安装要求用户具备本机的管理员权限。

OS Windows下的代理服务器安装

1. 按照创建Dr.Web代理服务器账户的描述通过Dr.Web安全管理中心创建代理服务器账户。
2. 将代理服务器需要了解的服务器的证书(见Dr.Web代理服务器连接Dr.Web服务器)、与服务器软件一起提供的代理服务器安装程序复制到安装代理服务器的工作站。
3. 启动代理服务器安装程序。打开**InstallShield Wizard**窗口，窗口显示要安装的产品信息。点击**下一步**。
4. 在代理服务器参数窗口的**常规**标签给出以下基本参数：
   - 如需可在软**件路径**一栏更改代理服务器所用文件的路径，包括运行日志、配置文件、缓存文件。默认使用路径`%PROGRAMDATA%/Doctor Web/drwcs`。更改路径需点击浏览。

- 在**监听地址**一栏给出代理服务器可监听的IP地址。默认情况下为any (0.0.0.0)——"监听"所有接口。



地址以网络格式输入，网络格式列于**附**录中的附录E. 网络地址特点。

- 在**端口**一栏给出代理服务器将监听的端口号。默认情况下为端口2193。
- 勾选**启用**发现启用服务器仿真模式。此模式允许客户端将代理服务器作为Dr.Web服务器进行多播搜索。
- 勾选**启用Multicasting**一项允许代理服务器响应发给服务器的广播请求。
  - 在**Multicast**组一栏给出代理服务器所属多播组的IP地址。代理服务器将监听给出的接口，以便在搜索处于活动状态的网络Dr.Web服务器时与客户端交互作用。如此栏为空，则代理服务器不被纳入任何一个多播组。默认服务器所在多播组是231.0.0.1。
- 在**与客户端的连接参数**部分：
  - 在**加密**下拉列表中选择代理服务器和其所服务的客户端间流量的加密模式，包括代理端和代理端安装程序。
  - 在压缩下拉列表中选择代理服务器和其所服务的客户端间流量的压缩模式，包括代理端和代理端安装程序。在**等级**一栏指定压缩等级（从1到9）。

5. 在**缓存**给出以下代理服务器缓存参数：

   勾选**启用缓存**，缓存代理服务器传输的数据并设置以下参数：

   - 在**校检删除周期（分钟）**指定缓存中校检数量超过**最大允许值**时对过时校检进行删除的时间间隔，以分钟计。默认为60分钟。
     - 在应**保存校检数量**指定清空后保留在缓存的每一产品校检最多数量。默认保留最新的3个校检，其他删除。
   - 在**卸载未使用文件的周期（以分钟计）**一栏指定从内存卸载未使用文件的时间间隔（单位为分钟）。默认值为10分钟。
   - 在**完整性检查模式**下拉列表选择缓存中数据完整性的检查模式：
     - **启动时**——启动代理服务器时（可能占用较长时间）。
     - **无操作时**——在代理服务器停工时。

   指定缓存设置后点击**下一步**。

6. 打开连接重定向设置的窗口：

   - 在**重定向地址**给出代理服务器向其重定向连接的服务器的地址。列表中的第一个服务器应是代理服务器连接后可获取配置的服务器。此服务器证书在步骤2已复制到工作站。



地址以网络格式输入，网络格式列于**附**录中的附录E. 网络地址特点。

   - 在**加密**下拉列表中选择代理代理服务器和指定的Dr.Web服务器间连接通道的流量加密模式。
   - 在压缩下拉列表中代理服务器和指定的Dr.Web服务器间连接通道的流量压缩模式。在**等级**下拉列表选择压缩等级（从1到9）。

   添加服务器需点击并给出上述设置。

   从此列表删除服务器需点击需要删除的服务器旁边的按钮。

完成代理服务器安装后代理服务器会连接此列表中的第一个服务器获取设置。

如服务器指定由代理服务器配置，则所有安装程序中给出的设置会改写为从服务器获取的设置。

完成重定向编辑后点击**下一步**。

7. 打开远程管理与Dr.Web服务器的连接的设置窗口。

   将连接流量重定向步骤6指定的第一个服务器。

   - 在**服务器证书**指示步骤2复制到工作站的证书文件。选择文件需点击**浏览**。
   - 在识别码和**密码**给出步骤1时在服务器创建的账户注册信息。

8. 打开准备安装代理服务器的通知窗口。

   如需更改安装高级参数，如代理服务器安装目录，需点击**高级参数**。

   开始安装代理服务器需点击**安装**按钮。

9. 安装过程结束后点击**退出**按钮。

10. 安装后代理服务器连接步骤6指定的第一个服务器获取完整的配置文件。如进行没有在服务器给出设置，则不会加载配置文件。将使用安装器给出的设置，直至所连接的服务器给出新设置。

OS UNIX下的代理服务器安装

1. 使用下列指令启动代理服务器安装程序：

   `./<软件版本>.tar.gz.run`

2. 继续安装请接受许可协议。
3. 指示服务器证书的路径。也可在完成服务器安装后再添加证书（参见Dr.Web代理服务器连接Dr.Web服务器）。
4. 如需可使用之前安装的代理服务器的配置文件：
   - 使用默认保存在`/var/tmp/drwcsd-proxy`目录的备份需点击ENTER。
   - 使用保存于另一目录的备份需手动输入备份路径。
   - 还可以不使用之前安装的代理服务器的配置文件，而是以默认设置安装代理服务器，操作是点击0。
5. 完成代理服务器安装后，如需可手动编辑相应的配置文件（参见Dr.Web代理服务器连接Dr.Web服务器）。

启动和停止

FreeBSD操作系统下软件安装过程中创建rc-脚本`/usr/local/etc/rc.d/dwcp_proxy`。请使用指令：

- `/usr/local/etc/rc.d/dwcp_proxy stop`——用于手动停止代理服务器；
- `/usr/local/etc/rc.d/dwcp_proxy start`——用于手动启动代理服务器。

Linux操作系统下软件安装过程中创建用于启动和停止代理服务器的`init`脚本`/etc/init.d/dwcp_proxy`。

5.4.4. Dr.Web代理服务器连接Dr.Web服务器

连接设置

将代理服务器连接到Dr.Web服务器必须具备：

- **服务器证书**drwcsd-certificate.pem。

  代理服务器连接并重定向客户端流量的所有服务器的证书。

  - 服务器证书用于连接服务器，以便远程管理设置，并支持服务器与代理服务器之间的流量加密。
  - 使用服务器证书和私钥签名的代理服务器证书（签名在与服务器建立连接后自动进行，不需要管理员参与），用于连接代理端，并支持代理端与代理服务器之间的流量加密。

  所有服务器证书保存在代理服务器的配置文件drwcsd-proxy-trusted.list，格式为（证书记录由一个或多个空行隔开）：

  ```
  [<证书_1>]


  [<证书_2>]


  [<证书_3>]

  ...
  ```

- **服务器地址。**

  代理服务器连接所有其配置文件指定的Dr.Web服务器，向其重定向客户端流量。但只从标志为控制服务器的服务器获得设置。如有多个服务器标为控制服务器，则依次连接所有服务器，直至第一次获取非空白配置。

- 访问**服务器的**识别码**和密**码。

  利用管理中心创建代理服务器账户后可以获得账户识别信息（见创建Dr.Web代理服务器账户）。

  > 代理服务器密码和识别码固定。需在代理服务器连接的所有服务器创建识别信息相同的代理服务器账户。

  识别信息保存在代理服务器配置文件drwcsd-proxy.auth，格式为：

  ```
  [<代理服务器ID>]

  [<代理服务器密码>]
  ```

将代理服务器连接到Dr.Web服务器

连接Dr.Web代理服务器必须在Dr.Web服务器端启用相应的协议。操作是在Dr.Web管理中心的**管理** → **模块**部分勾选**Dr.Web代理服务器**协议，保存设置后重启服务器。

OS Windows下安装时自动连接：

- 如在安装代理端过程中或在安装有代理端的工作站安装代理服务器，则自动连接服务器。
- 如通过OS Windows图形安装程序安装代理服务器，则使用管理员在安装程序指定的连接参数自动连接服务器。

  安装代理服务器后用于连接服务器的文件默认位于目录：`C:\Program Files\DrWeb Server\etc`。

UNIX® 家族操作系统下安装时需手动：

1. 按照利用安装程序安装Dr.Web代理服务器的描述安装OS UNIX代理服务器。
2. 按照创建Dr.Web代理服务器账户的描述通过Dr.Web安全管理中心创建代理服务器账户。
3. 将服务器证书复制到安装代理服务器的电脑。
4. 在配置文件`drwcsd-proxy-trusted.list`指示在步骤3复制到电脑的证书：将证书文件内容复制后按照见上格式粘贴到配置文件。
5. 在配置文件`drwcsd-proxy.auth`为步骤2创建的账户按照见上格式指定连接服务器的设置。

   文件`drwcsd-proxy-trusted.list`和`drwcsd-proxy.auth`应位于以下目录：

   - OS Linux：`/var/opt/drwcs/etc`
   - OS FreeBSD：`/var/drwcs/etc`

   需为这些文件给出以下权限：

```
drwcsd-proxy-trusted.list 0644 drwcs:drwcs

drwcsd-proxy.auth 0600 drwcs:drwcs
```

第六章、删除Dr.Web Enterprise Security Suite组件

6.1. 卸载Dr.Web服务器

6.1.1. OS Windows下Dr.Web服务器的卸载

卸载Dr.Web服务器软件或Dr.Web安全管理中心插件需启动相应产品的安装包，版本应与安装使用的安装包相同。安装程序会自动确定软件产品并建议将其删除。删除软件需点击**删除**。

卸载Dr.Web服务器软件还可以使用Windows操作系统的常规方式：**控制面板** → **添加/删除程序**。



卸载服务器时进行配置文件、加密密钥和数据库备份，前提是设置了**保存Dr.Web服务器关键数据备份**功能。

6.1.2. UNIX家族操作系统Dr.Web服务器的卸载



所有卸载操作都应使用超级管理员（**root**）账户进行。

删除版本10和更高版本Dr.Web服务器的操作

服务器操作系统	操作
FreeBSD	启动脚本： `/usr/local/etc/drweb.com/software/drweb-esuite.remove`
Linux	启动脚本： `/etc/opt/drweb.com/software/drweb-esuite.remove`



OS **FreeBSD**和OS **Linux**下卸载服务器会自动停止服务器进程，数据库、密钥文件和配置文件会自动拷贝到默认目录`/var/tmp/drwcs`（备份文件列表见UNIX家族操作系统Dr.Web服务器的更新）。

取消备份需要声明环境变量`SKIP_BACKUP`。变量可为任意值。如：`SKIP_BACKUP="x"`

也可将此变量定义添加到文件`common.conf`。

6.2. 删除Dr.Web代理端

从受保护工作站删除Dr.Web代理端的可选方式：

- OS Windows工作站：
  - 利用管理中心通过网络删除。
  - 在工作站本地删除。
  - 利用Active Directory服务，如安装代理端使用的是这一服务。
- OS Android、OS Linux、macOS工作站：在本地进行。

在OS Android、OS Linux、macOS工作站本地删除Dr.Web代理端介绍参见相应操作系统的**用户手册**。

6.2.1. 删除OS Windows下的Dr.Web代理端

远程删除Dr.Web代理端和反病毒软件包

代理端软件的远程安装和卸载只能在局域网内进行，并要求具备该局域网的管理员权限。

如果使用管理中心删除代理端和反病毒软件包，则不会从工作站上删除隔离区。

远程卸载反病毒工作站软件的操作（只适用于 Windows 家族操作系统）

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在打开的窗口的反病毒网络目录中选择需要的组或个别反病毒工作站。
3. 在反病毒网络目录工具面板中点击**常规** → **卸载Dr.Web代理端**。
4. 代理端软件和反病毒软件包将从所选工作站上删除。

如果下达运行删除进程的命令时Dr.Web服务器和反病毒工作站之间没有连接，则连接一恢复代理端软件就会从所选工作站上删除。

远程删除代理端（在工作站以背景模式进行删除），将强制重启工作站，时间间隔为5分钟，无法更改时间间隔或取消重启。工作站会出现弹出窗口通知用户会重启。

本地删除Dr.Web代理端和反病毒软件包



本地删除代理端和反病毒软件包在服务器的权限部分允许此项的情况下才能进行（参见管理员手册的设置用户权限）。

删除工作站上的反病毒软件（代理端和反病毒软件包）可通过两种方式：

1. 使用Windows操作系统的常规工具。
2. 使用代理端安装程序。



如果使用Windows操作系统常规工具或代理端安装程序来删除代理端和反病毒软件包，则会提示用户是否删除隔离区。

使用 Windows 操作系统的卸载服务进行卸载



只有在利用图形模式安装代理端时选择了**在已安装程序列表中注册Dr.Web代理端**的情况下才能使用此方式进行卸载。

如果代理端是以安装程序背景模式安装的，则只有在安装时使用了 `/regagent yes`参数的情况下才能使用操作系统的常规工具卸载反病毒软件。

使用Windows操作系统的常规工具删除代理端和反病毒软件包需使用 **控制面板** → **添加或删除程序**（详细操作见 Windows操作系统Dr.Web代理端**用户手册**）。

使用安装程序进行卸载

- **客户模块win-es-agent-setup.exe**

  使用代理端安装过程中创建的客户端模块删除代理端软件和反病毒软件包，需使用参数`/instMode remove`启动安装文件`win-es-agent-setup.exe`。如需监控删除进程，还需使用参数`/silent no`。

  安装文件 `win-es-agent-setup.exe`默认位置：

  - OS Windows XP 和OS Windows Server 2003：
    `%ALLUSERSPROFILE%\Application Data\Doctor Web\Setup\`
  - OS Windows Vista或更高版本和OS Windows Server 2008或更高版本：
    `%ALLUSERSPROFILE%\Doctor Web\Setup\`

  如Windows 7中`%ALLUSERPROFILE%`对应`C:\ProgramData`：

  ```
  C:\ProgramData\Doctor Web\Setup\win-es-agent-setup.exe /instMode
  remove /silent no
  ```

- **个人安装包drweb_ess_*<OS>*_*<工作站>*.exe**

  如利用安装包删除对代理端软件和反病毒软件包需要运行与所安装的产品同版本的安装文件 `drweb_ess_<OS>_<工作站>.exe`。

- **完整安装包drweb-12.0.0-*<编号>*-esuite-agent-full-windows.exe**

  如利用完整安装程序删除对代理端软件和反病毒软件包需要运行与所安装的产品同版本的安装文件drweb-12.0.0-*<编号>*-esuite-agent-full-windows.exe。

- **网络安装程序drwinst.exe**

  使用网络安装程序在工作中本地删除代理端软件和反病毒软件包，需在Dr.Web代理端安装文件夹（默认为C:\Program Files\DrWeb）使用参数/instMode remove启动安装程序drwinst.exe。如需监控删除进程，还需使用参数/silent no。

  例如：

```
drwinst /instMode remove /silent no
```

> 启动安装包 drweb_ess_*<OS>*_*<工作站>*.exe，完整安装程序drweb-12.0.0-*<编号>*-esuite-agent-full-windows.exe和网络安装程序drwinst.exe时会启动客户端模块 win-es-agent-setup.exe，由此模块执行删除操作。
>
> 无参数启动客户端模块win-es-agent-setup.exe时会确定已安装的产品并以更改/删除模式启动。如直接以删除模式启动，需使用参数/instMode remove。

6.2.2. 通过Active Directory服务删除代理端

> 删除代理端在服务器的权限部分允许此项的情况下才能进行（参见管理员手册的设置用户权限）。

1. 在Windows操作系统控制面板选择**管理工具**中的**Active Directory – 用户和计算机**。
2. 在域选择您所创建的组织单位**ESS**。在菜单中选择**属性**。打开**ESS属性**窗口。
3. 进入组**策略**标签。选择名称为**ESS策略**的列表项。然后双击此项打开组**策略**对象编辑窗口。
4. 在分层列表中选择计**算机配置** → **软件配置** → **软件安装** → **软件包**。之后在代理端软件包菜单选择**所有任务** → **删除** → **确定**。
5. 在组**策略**标签点击**确定**。
6. Dr.Web代理端将在计算机下一次在域中注册时被删除。

6.3. 删除Dr.Web代理服务器

可利用下列一种方式删除代理服务器：

1. 本地方式。

   本地删除是管理员在安装代理服务器的电脑直接进行删除。

2. 远程。

   远程删除代理服务器是在管理中心通过局域网来进行删除，前提是代理服务器连接服务器。

6.3.1. 本地删除Dr.Web代理服务器

OS Windows下



删除代理服务器时会删除配置文件drwcsd-proxy.conf（版本10和更低版本为drwcsd-proxy.xml）。如需可在删除代理服务器前手动保存配置文件。

删除代理服务器软件使用Windows操作系统常规工具，利用**控制面板** →**添加或删除程序**（OS Windows 2008以及更高版本为**程序和组件**）。

UNIX家族操作系统



删除代理服务器时自动将配置文件备份保存到目录/var/tmp/drwcsd-proxy。

代理服务器软件	操作
FreeBSD	启动脚本： /usr/local/etc/drweb.com/software/drweb-esuite-proxy.remove
Linux	启动脚本： /etc/opt/drweb.com/software/drweb-proxy.remove

6.3.2. 远程删除Dr.Web代理服务器

远程删除代理服务器的前提是代理服务器连接服务器（见Dr.Web代理服务器连接Dr.Web服务器）。



在管理中心删除代理服务器账户时代理服务器本身从工作站卸载。

删除代理服务器的操作

1. 在管理中心主菜单选择**反病毒网络**一项。
2. 在打开窗口的分层列表选择需要删除的一个或几个代理服务器。
3. 在工具面板点击**常规** → **删除所选对象**。
4. 打开确认删除对象窗口。点击**确定**按钮。

删除安装在相邻工作站的代理服务器的操作

1. 在管理中心主菜单选择**反病毒网络**一项。

2. 用以下方式打开安装代理服务器的工作站属性页面：
   a) 点击反病毒网络分层列表中的工作站名称。在管理中心窗口右侧会自动打开工作站属性。
   b) 选择控制菜单的**属性**一项。打开工作站属性窗口。
3. 在工作站属性窗口转至**代理服务器**部分。
4. 点击**删除代理服务器**。
5. 点击**保存**。代理服务器从工作站卸载。代理服务器账户从服务器删除。

第七章、更新Dr.Web Enterprise Security Suite组件

版本11.X至12.0的更新可利用管理中心进行。操作介绍见**管理员手册**更新更新Dr.Web服务器和利用备份还原。

在开始更新Dr.Web Enterprise Security Suite 及其组件前需注意以下事项：

- 在更新之前务请检查访问互联网的TCP/IP协议设置是否正确，特别需要注意DNS服务是否开启，其设置是否正确。
- 在更新Dr.Web服务器前建议先将包括Dr.Web代理端在内的Dr.Web Enterprise Security Suite反病毒网络的所有组件更新GUS上的最新版本。
- 多服务器反病毒网络中必须注意服务器版本12和服务器版本6之间不能传递服务器间更新，服务器间连接只用于传递统计信息。传递服务器间更新必须更新所有服务器。如果由于存在安装于其操作系统版本12不支持的工作站的代理端（参见更新Dr.Web代理端）而必须保留老版本的服务器，则服务器版本6和服务器版本12应分别更新。
- 将Dr.Web服务器群集从版本6和版本10升级至版本12时必须分别进行升级，也就是需要依次将各节点脱离群集，转至内设数据库后进行升级，然后再逐一重返群集。
- 使用Dr.Web代理服务器的反病毒网络在将组件更新至版本12.0时必须将Dr.Web代理服务器也更新至版本12.0。否则12.0版本提供的代理端将无法连接版本12.0的服务器。建议更新次序为：Dr.Web服务器 → Dr.Web代理服务器 → Dr.Web代理端。
- 将服务器从版本6更新至版本12时，不保存通过代理服务器的 服务器运行设置。安装版本12后需手动设置代理服务器连接（参见**管理员手册**的代理服务器）。
- 升级服务器时库的所有设置都不会转至新版本（均归为默认设置），但会进行备份。必要时在服务器升级后手动指定库设置。
- 将服务器更新至版本12时库产品**用于Android操作系统的Dr.Web代理端**、**用于UNIX操作系统的Dr.Web代理端**和**Dr.Web代理服务器**默认情况下只在工作站申请更新这些产品后才会更新。参见**管理员手册**，中的库详细配置。

  如果您使用的服务器未接通互联网，而是手动从另一服务器或利用库加载器加载更新，则在安装或更新在库设置中为其启用了**只在接到申请时更新**选项的产品前必须手动将这些产品加载到库中。

7.1. OS Windows下Dr.Web服务器的更新

服务器从版本6、10和11更新至版本12和在版本12内的更新由安装程序自动完成。

版本11.X至12.0的更新还可利用管理中心进行。操作介绍见**管理员手册**更新更新Dr.Web服务器和利用备份还原。

从版本10或更低版本升级Windows操作系统的Dr.Web服务器时管理中心Web服务器以下部分的设置不会转至版本12：

- **Dr.Web服务器配置** → **网络** → **加载**（文件`download.conf`），
- 远程访问**Dr.Web服务器**（文件`frontdoor.conf`），
- **Web服务器配置**（文件`webmin.conf`）。

这几部分的设置将还原为默认设置。如果要使用上一版本的设置，需在服务器升级后在管理中心的相应部分根据配置文件备份进行手动设置。

更新服务器前请注意Dr.Web代理端更新部分。

在版本12内的更新还可利用管理中心进行。操作介绍见**管理员手册**更新更新Dr.Web服务器和利用备份还原。

并非所有版本12以内的服务器更新含有软件文件。某些文件只能通过管理中心安装。

保存配置文件

利用安装程序更新服务器至版本12时配置文件自动保存到为备份指定的目录：

- 从版本6更新时：在目录 *<安装磁盘>*:\DrWeb Backup。
- 从版本10、11和在版本12内更新时：是**保存Dr.Web服务器关键数据**备份设置中指定的目录（默认为*<安装磁盘>*:\DrWeb Backup）。

从服务器版本6更新时保存以下配置文件：

文件	描述
agent.key（文件名称可能有区别）	代理端授权密钥
auth-ads.xml	通过Active Directory进行管理员外部身份验证的配置文件
auth-ldap.xml	通过LDAP进行管理员外部身份验证的配置文件
auth-radius.xml	通过RADIUS进行管理员外部身份验证的配置文件
drwcsd.conf（文件名称可能有区别）	服务器配置文件
dbinternal.dbs	内设数据库
drwcsd.pri	加密私钥
drwcsd.pub	加密公钥
enterprise.key（文件名称可能有区别）	服务器授权密钥
webmin.conf	管理中心配置文件

从服务器版本10 更新时保存以下配置文件：

文件	描述
agent.key（文件名称可能有区别）	代理端授权密钥
auth-ads.xml	通过Active Directory进行管理员外部身份验证的配置文件
auth-ldap.xml	通过LDAP进行管理员外部身份验证的配置文件
auth-radius.xml	通过RADIUS进行管理员外部身份验证的配置文件
enterprise.key（文件名称可能有区别）	服务器授权密钥。从较早版本升级时如存在则保存此密钥。安装新的服务器12.0时没有
drwcsd.conf（文件名称可能有区别）	服务器配置文件
drwcsd.conf.distr	服务器默认参数配置文件模板
drwcsd.pri	加密私钥
drwcsd.pub	加密公钥
download.conf	形成代理端安装包的网络设置
frontdoor.conf	用于服务器远程诊断工具的配置文件
webmin.conf	管理中心配置文件
openssl.cnf	服务器HTTPS证书

从版本11和在版本12内更新服务器时保存以下配置文件：

文件	描述
agent.key（文件名称可能有区别）	代理端授权密钥
auth-ads.conf	通过Active Directory进行管理员外部身份验证的配置文件
auth-radius.conf	通过RADIUS进行管理员外部身份验证的配置文件
auth-ldap.conf	通过LDAP进行管理员外部身份验证的配置文件
auth-ldap-rfc4515.conf	通过LDAP进行管理员外部身份验证的配置文件，采用简易方式
auth-ldap-rfc4515-check-group.conf	通过LDAP采用简易方式进行管理员外部身份验证的配置文件模板，检查是否属于Active Directory组

文件	描述
auth-ldap-rfc4515-check-group-novar.conf	通过LDAP采用简易方式进行管理员外部身份验证的配置文件模板，检查是否属于Active Directory组，并使用变量
auth-ldap-rfc4515-simple-login.conf	通过LDAP采用简易方式进行管理员外部身份验证的配置文件模
auth-pam.conf	通过PAM进行管理员外部身份验证的配置文件
enterprise.key(文件名称可能有区别)	服务器授权密钥。从较早版本升级时如存在则保存此密钥。安装新的服务器12.0时没有
drwcsd-certificate.pem	服务器证书
download.conf	形成代理端安装包的网络设置
drwcsd.conf(文件名称可能有区别)	服务器配置文件
drwcsd.conf.distr	服务器默认参数配置文件模板
drwcsd.pri	加密私钥
dbexport.gz	导出数据库
drwcsd.pub	加密公钥
frontdoor.conf	用于服务器远程诊断工具的配置文件
openssl.cnf	服务器HTTPS证书
webmin.conf	管理中心配置文件
yalocator.apikey	插件Yandex.Locator的API密钥



如果计划使用服务器版本6的配置文件，请注意：

1. 服务器授权密钥已不再使用(参见 授权)。
2. 内设数据库进行更新，而服务器配置文件由安装程序转换。在时这些文件不会替换为从服务器版本6升级时自动保存的备份。

必要时可将服务器其他重要文件保存至有别于安装目录的另一目录，例如\var\templates目录中的报告模板。

保存数据库



数据库MS SQL CE自Dr.Web服务器10起不再支持。利用安装程序自动更新服务器时自动将MS SQL CE 数据库转换为内设数据库SQLite。

更新前请确认在Microsoft SQL DBMS创建新数据库时指定了排序需考虑大小写（后缀_CS）和区别标记（后缀_AS）。否则将无法自动更新。

更新前倾确认Dr.Web服务器版本12支持您所使用的DBMS。否则将无法自动更新。支持的DBMS列表见**附**录中的附录B. DBMS使用设置。DBMS驱动程序参数。

建议在更新Dr.Web Enterprise Security Suite软件前进行数据库备份。

保存数据库

1. 停止服务器运行。
2. 将数据库导出到文件：

```
"C:\Program Files\DrWeb Server\bin\drwcsd.exe" -home="C:\Program
Files\DrWeb Server" -var-root="C:\Program Files\DrWeb Server\var" -
verbosity=all exportdb <备份目录>\esbase.es
```

如服务器使用的是外设数据库，建议使用与数据库同时供货的标准工具进行备份。

请确认Dr.Web Enterprise Security Suite 数据库已成功导出。如出现异常情况，没数据库备份就无法恢复服务器。

更新Dr.Web服务器

更新Dr.Web服务器需启动程序文件。之后的步骤取决于要更新的是什么版本。

安装程序默认语言为操作系统语言。如需可在安装任一帮助点击安装程序右上角的相应选项更改语言。

如使用的是服务器外设数据库，更新过程中也需选择**使用**现**数据**库。

如果计划使用ODBC接通Oracle作为外设数据库，则在安装（更新）服务器时，需在安装程序设置中取消安装Oracle DBMS内置客户端（在**支持数据**库 → **Oracle数据**库驱动**程序**）。

否则将出现库冲突而无法通过ODBC使用Oracle数据库。

从版本6更新时

1. 打开已安装有服务器软件上一版本的通知窗口，同时显示更新至新版本的简短说明。开始设置更新进程需点击**更新**按钮。
2. 打开包含产品信息及许可协议条款链接的窗口。了解许可协议条件继续安装需选择**我接受**许可协议**的条款**并点击**下一步**按钮。

3. 以下步骤是对服务器的设置，与使用上一版本配置文件安装Dr.Web服务器类似。安装程序自动确定服务器安装目录、上次安装的配置文件和内置数据库位置。如需可更改安装程序自动搜索到的文件的路径。
4. 点击**安装**按钮开始卸载前一版本的服务器，开始安装12.0版本服务器。

   删除服务器过程中配置文件自动保存到目录*<安装磁盘>*:\DrWeb Backup。

从版本10.0更新时

1. 打开已安装有服务器软件上一版本的通知窗口，同时显示更新至新版本的简短说明。开始设置更新进程需点击**更新**按钮。
2. 打开包含产品信息及许可协议条款链接的窗口。了解许可协议条件继续安装需选择**我接受许可协议的条款**并点击**下一步**按钮。
3. 以下步骤是对服务器的设置，与使用上一版本配置文件安装Dr.Web服务器类似。安装程序自动确定服务器安装目录、上次安装的配置文件和内置数据库位置。如需可更改安装程序自动搜索到的文件的路径。
4. 点击**安装**按钮开始卸载前一版本的服务器，开始安装12.0版本服务器。
5. 更新过程中打开删除老版本服务器前重大数据备份设置窗口。建议勾选**保存Dr.Web服务器关键数据备份**。如需可更改备份的默认目录(*<安装磁盘>*:\DrWeb Backup)。

从版本10.0.1、10.1、11更新和在版本12内更新时

1. 打开已安装有服务器软件上一版本的通知窗口，同时显示更新至新版本的简短说明。开始设置更新进程需点击**更新**按钮。
2. 打开删除老版本服务器前重大数据备份设置窗口。建议勾选**保存Dr.Web服务器关键数据备份**。如需可更改备份的默认目录(*<安装磁盘>*:\DrWeb Backup)。开始删除老版本服务器需点击**删除**。
3. 删除代理服务器老版本后开始安装新版本。打开包含产品信息及许可协议条款链接的窗口。了解许可协议条件继续安装需选择**我接受许可协议的条款**并点击**下一步**按钮。
4. 以下步骤是对服务器的设置，与使用上一版本配置文件安装Dr.Web服务器类似。安装程序自动确定服务器安装目录、上次安装的配置文件和内置数据库位置。如需可更改安装程序自动搜索到的文件的路径。
5. 开始安装服务器版本12.0需点击**安装**按钮。



结束反病毒网络服务器更新后必须：

1. 重新设置邻居服务器的流量加密和压缩(参见**管理员手册**的设置Dr.Web服务器间连接)。
2. 清空登录管理中心所使用的web浏览器的缓存。

7.2. UNIX家族操作系统Dr.Web服务器的更新

如将服务器更新至版本12.0取决于原来是什么版本：

- 从6.0.4更新至版本12.0只能手动进行。
- 利用安装程序将版本10.X的服务器自动更新至版本12.0时，并非所有UNIX家族操作系统都可以进行覆盖安装。因此对于无法进行覆盖安装而自动更新的UNIX家族操作系统需首先备份，必须手动更新。

- 从11.X版本和在版本12.0范围内更新服务器，对于相同类型的安装包，所有UNIX家族操作系统都可利用安装程序自动更新。如需可以进行手动更新。
- 版本11.X至12.0的更新还可利用管理中心进行。操作介绍见**管理员手册**更新更新Dr.Web服务器和利用备份还原。



从版本10或更低版本升级UNIX家族操作系统的Dr.Web服务器时管理中心**Web服务器配置**部分的设置（文件`webmin.conf`）不会转至版本12。

这部分的设置将还原为默认设置。如果要使用上一版本的设置，需在服务器升级后在管理中心的相应部分根据配置文件备份进行手动设置。

所有更新操作都应使用超级管理员**root**账户进行。

更新服务器前请注意Dr.Web代理端更新部分。



在版本12内的更新还可利用管理中心进行。操作介绍见**管理员手册**更新更新Dr.Web服务器和利用备份还原。

并非所有版本12以内的服务器更新含有软件文件。某些文件只能通过管理中心安装。

保存配置文件

删除和自动更新服务器至版本12时以下配置文件自动保存到为备份指定的默认目录：`/var/tmp/drwcs/`。

删除服务器版本6时保存以下配置文件：

文件	描述
`agent.key`（文件名称可能有区别）	代理端授权密钥
`certificate.pem`	SSL证书
`common.conf`	配置文件（用于某些UNIX家族操作系统）
`dbinternal.dbs`	内设数据库
`drwcsd.conf`（文件名称可能有区别）	服务器配置文件
`drwcsd.pri`	加密私钥
`drwcsd.pub`	加密公钥
`enterprise.key`（文件名称可能有区别）	服务器授权密钥

文件	描述
private-key.pem	RSA私钥
webmin.conf	管理中心配置文件

删除服务器版本10时保存以下配置文件：

文件	描述
agent.key（文件名称可能有区别）	代理端授权密钥
auth-ldap.xml	通过LDAP进行管理员外部身份验证的配置文件
auth-pam.xml	通过PAM进行管理员外部身份验证的配置文件
auth-radius.xml	通过RADIUS进行管理员外部身份验证的配置文件
certificate.pem	SSL证书
common.conf	配置文件（用于某些UNIX家族操作系统）
dbexport.gz	导出数据库（在通过指令drwcs.sh xmlexportdb删除服务器过程只创建）
download.conf	形成代理端安装包的网络设置
drwcsd.conf（文件名称可能有区别）	服务器配置文件
drwcsd.pri	加密私钥
drwcsd.pub	加密公钥
enterprise.key（文件名称可能有区别）	服务器授权密钥。从较早版本升级时如存在则保存此密钥。安装新的服务器12.0时没有
frontdoor.conf	用于服务器远程诊断工具的配置文件
local.conf	服务器日志设置
private-key.pem	RSA私钥
webmin.conf	管理中心配置文件
*.dbs *.sqlite	内设数据库

删除服务器版本11和12时保存以下配置文件：

文件	描述
agent.key（文件名称可能有区别）	代理端授权密钥
auth-ldap.conf	通过LDAP进行管理员外部身份验证的配置文件
auth-ldap-rfc4515.conf	通过LDAP进行管理员外部身份验证的配置文件，采用简易方式。
auth-pam.conf	通过PAM进行管理员外部身份验证的配置文件
auth-radius.conf	通过RADIUS进行管理员外部身份验证的配置文件
certificate.pem	SSL证书
common.conf	配置文件（用于某些UNIX家族操作系统）
dbexport.gz	导出数据库（在通过指令drwcs.sh xmlexportdb删除服务器过程只创建）
download.conf	形成代理端安装包的网络设置
drwcsd-certificate.pem	服务器证书
drwcsd.conf（文件名称可能有区别）	服务器配置文件
drwcsd.pri	加密私钥
drwcsd.pub	加密公钥
enterprise.key（文件名称可能有区别）	服务器授权密钥。从较早版本升级时如存在则保存此密钥。安装新的服务器12.0时没有
frontdoor.conf	用于服务器远程诊断工具的配置文件
local.conf	服务器日志设置
private-key.pem	RSA私钥
webmin.conf	管理中心配置文件
yalocator.apikey	插件Yandex.Locator的API密钥

自动更新时备份目录还保存以下文件：

服务器版本10：

文件	描述
auth-ldap.xml	通过LDAP进行管理员外部身份验证的配置文件
auth-pam.xml	通过PAM进行管理员外部身份验证的配置文件
auth-radius.xml	通过RADIUS进行管理员外部身份验证的配置文件
db.backup.gz	导出数据库（在通过指令drwcs.sh exportdb更新服务器过程只创建）

对于服务器版本11和12：

文件	描述
auth-ldap.conf	通过LDAP进行管理员外部身份验证的配置文件
auth-ldap-rfc4515.conf	通过LDAP进行管理员外部身份验证的配置文件，采用简易方式。
auth-pam.conf	通过PAM进行管理员外部身份验证的配置文件
auth-radius.conf	通过RADIUS进行管理员外部身份验证的配置文件
db.backup.gz	导出数据库（在通过指令drwcs.sh exportdb更新服务器过程只创建）

如果计划使用服务器版本6的配置文件，请注意：

1. 服务器授权密钥已不再使用（参见 授权）。
2. 内设数据库进行更新，而服务器配置文件由安装程序转换。在时这些文件不会替换为从服务器版本6升级时自动保存的备份。

保存数据库

建议在更新Dr.Web Enterprise Security Suite软件前进行数据库备份。

保存数据库

1. 停止服务器运行。
2. 将数据库导出到文件：
   - OS FreeBSD：
     ```
     # /usr/local/etc/rc.d/drwcsd exportdb /var/tmp/esbase.es
     ```
   - OS Linux：
     ```
     # /etc/init.d/drwcsd exportdb /var/tmp/esbase.es
     ```

如服务器使用的是外设数据库，建议使用与数据库同时供货的标准工具进行备份。



请确认Dr.Web Enterprise Security Suite 数据库已成功导出。如出现异常情况，没数据库备份就无法恢复服务器。

自动更新

将服务器从版本10更新至12版本（除了从安装包*.rpm.run和*.deb.run安装的OS **Linux**服务器），可以不必删除老版本和安装服务器新版本，而是自动进行数据包更新。操作是启动安装服务器的相应数据包。

从版本11和在版本12范围内更新服务器，对于相同类型的安装包，所有UNIX家族操作系统都为自动更新。

这时所有自动保存的配置文件将自动转换后移至相应的目录。还会保存备份目录中的某些配置文件。

手动更新

如无法将6.0.4或更高版本的服务器覆盖更新已安装的软件包，需先备份后删除较早版本的服务器软件，再在保存的备份的基础上安装12版本软件。

更新Dr.Web服务器的操作

1. 停止服务器运行。
2. 如以后要使用某些文件（除了在删除服务器时在步骤**3**自动保存的文件以外），需手动建立这些文件的备份，如报告模板等等。
3. 删除服务器软件（参见UNIX家族操作系统Dr.Web服务器的卸载）。这时将自动提示保存文件备份。只需输入路径或确认默认路径。
4. 使用步骤**3**生成的备份按照常规操作（参见UNIX家族操作系统下Dr.Web服务器的安装）安装Dr.Web服务器版本12.0。所有保存的配置文件和内设数据库将自动转换，供服务器12.0版本使用。不经自动转换无法使用老版本服务器的数据库（如使用的是内设数据库）和某些配置文件。

   如在删除服务器前手动保存了某些文件，需将这些文件移至其在前一版本服务器上所处的目录。



所有从上一版本服务器保存的文件（参见步骤4）的文件所有人必须设为安装新版本服务器时选择的用户文件所有人（默认为**drwcs**）。

5. 启动服务器。
6. 设置库更新并全部更新库。



结束反病毒网络服务器更新后必须重新设置邻居服务器的流量加密和压缩（参见**管理员手册**的设置Dr.Web服务器间连接）。

7.3. 更新Dr.Web代理端

更新服务器软件后更新代理端的相应介绍：

1. OS Windows工作站Dr.Web代理端的更新，
2. OS Android工作站Dr.Web代理端的更新，
3. OS Linux和macOS工作站Dr.Web代理端的更新。

7.3.1. OS Windows工作站Dr.Web代理端的更新

更新Dr.Web Enterprise Security Suite 10中提供的代理端

Dr.Web Enterprise Security Suite 10中提供的代理端为自动更新。

工作站自动更新后出现必须重启的通知窗口；管理中心的工作站状态标记为更新后必须重启。结束更新后本地重启工作站或通过管理中心远程重启。

如工作站是通过Dr.Web代理服务器版本10或更早版本连接服务器，在更新代理端前必须将代理服务器更新至版本12或删除代理服务器。

自动更新Dr.Web Enterprise Security Suite 6中提供的代理端

可以进行自动更新的前提条件：

1. 代理端所安装的计算机的Windows操作系统应是 Dr.Web Enterprise Security Suite版本12.0支持的安装代理端的操作系统（参见附录的附录A. 产品支持的所有操作系统列表）。
2. 取决于服务器的设置，执行自动更新时存在以下几种方案：
   a) 自动更新可进行，如更新服务器是保留了原服务器的加密密钥和网络设置。
   b) 自动更新时需进行手动设置，如更新服务器是指定了新的服务器加密密钥和网络设置。



自动更新过程中需注意以下事项：

1. 删除代理端后不显示必须重启工作站的通知。管理员需自行重启。
2. 在删除代理端老版本和安装新版本期间工作站没有反病毒保护。
3. 更新代理端后如不重启工作站，反病毒软件功能会受到显著，不能为工作站提供全面的反病毒保护。用户必须按照代理端提示重启工作站。

代理端自动更新的流程：

1. 启动更新后删除老版本的代理端。
2. 手动进行工作站重启。
3. 安装新版本的代理端。服务器日程自动创建任务。
4. 完成代理端更新后，工作站自动连接服务器。管理中心状态部分已更新的工作站会显示必须重启通知。必须重启工作站。

需手动设置的代理端自动更新的流程：

1. 手动更改连接新服务器的设置，更换工作站上的加密公钥。
2. 更改工作站设置后工作站连接到服务器，启动代理端更新进程。
3. 启动更新后删除老版本的代理端。
4. 手动进行工作站重启。
5. 安装新版本的代理端。服务器日程自动创建任务。
6. 完成代理端更新后，工作站自动连接服务器。管理中心状态部分已更新的工作站会显示必须重启通知。必须重启工作站。

手动更新Dr.Web Enterprise Security Suite 6中提供的代理端

如因某种原因自动更新时未能安装新版本的代理端，不会重新尝试安装。反病毒软件不会安装到工作站，这样的工作站在管理中心讲显示为离线工作站。

这时需手动进行代理端安装。完成代理端安装后需在管理中心的反病毒网络分层列表合并老工作站和新工作站。

不支持更新

如代理端所安装的计算机的操作系统不是Dr.Web Enterprise Security Suite版本12.0支持的安装代理端的操作系统，不会进行任何更新操作。

代理端如果安装在不支持的操作系统，不能从新服务器获得更新（包括病毒库更新）。如果必须保留安装于不支持的操作系统的代理端，需在反病毒网络保留这些代理端连接的老版本的服务器。这时服务器版本6和服务器版本12.0应分别获取更新。



执行局域网重要功能的工作站上如何更新代理端的建议见附录的局域网服务器上的代理端更新。

7.3.2. OS Android工作站Dr.Web代理端的更新



与Dr.Web Enterprise Security Suite版本12.0交互作用需在移动设备手动更新Dr.Web for Android代理端。

Dr.Web Enterprise Security Suite版本12.0只支持Dr.Web for Android代理端12.2和更高版本。

可选择以下一种方式本地更新用于Android操作系统的Dr.Web代理端

1. 如果可以从互联网下载单机版本代理端的安装包。

   更新Dr.Web服务器前在移动设备手动将Dr.Web for Android代理端更新到版本12.2或更高版本。可从Doctor Web公司官网下载新版本，地址为https://download.drweb.com/android/。新代理端连接上一版本服务器后按常规操作将服务器更新至版本12.0。

2. 如无法从互联网下载单机版本代理端的安装包。

   Dr.Web服务器更新后Dr.Web for Android代理端自动连接更新后的服务器。尝试更新时会因病毒库版本不符而中断移动设备的保护。直接在移动设备手动更新代理端。可在管理中心工作站属性或安装页面下载代理端新版本安装包。

3. 如无法从互联网下载单机版本代理端的安装包，且不希望移动设备出现更新错误。

   Dr.Web服务器更新前断开Dr.Web for Android代理端，这样移动设备就不会连接新服务器下载不兼容的更新。按常规操作将服务器更新至版本12.0。在管理中心工作站属性或安装页面下载代理端新版本安装包，在移动设备手动更新代理端。将更新后的代理端连接新服务器。

7.3.3. OS Linux和macOS工作站Dr.Web代理端的更新

安装于OS Linux和macOS工作站的代理端能够连接服务器版本12.0的前提是：

1. 代理端所安装的计算机的操作系统应是Dr.Web Enterprise Security Suite版本12.0支持的安装代理端的操作系统（参见**附录**的附录A. 产品支持的所有操作系统列表）。
2. 工作站应指定由更新后服务器的加密密钥和网络设置。

工作站连接到更新后的服务器后：

1. 只在工作站更新病毒库。不会自动更新反病毒软件包。
2. 如在工作站安装的是最新版本的软件，则不需要进行任何操作。
3. 如工作站安装的是老版本软件，需在管理中心工作站属性或安装页面下载代理端新版本安装包。按照**用户指南**手动更新工作站软件。

7.4. 更新Dr.Web代理服务器

7.4.1. 在运行过程中更新Dr.Web代理服务器

可在运行过程中自动更新Dr.Web代理服务器。



如果UNIX家族操作系统Dr.Web服务器之前是从版本11.0或11.0.1进行的升级，则无法自动更新Dr.Web代理服务器。取消这一限制需在**管理**→库详细**配置**→**Dr.Web代理服务器**→**同步的只更新以下文件**手动删除后缀`^win.*`。

如果一开始安装的就是Dr.Web服务器版本11.0.2，则没有对代理服务器自动更新的限制。

更新日程取决于代理服务器预缓存的设置：

1. 如果代理服务器未列入预缓存列表（包括不启用缓存的情况），则会按照自动更新日程加载和安装代理服务器更新。
2. 如果代理服务器已列入预缓存列表，则会按照预缓存日程日程加载代理服务器更新。获得代理服务器新校检后会按照自动更新日程转至新校检。

可使用以下一种方式设置自动更新：

- 在控制服务器管理中心代理服务器设置的**更新**部分。详见**管理员手册**中的远程设置代理服务器。

- 通过代理服务器配置文件drwcsd-proxy.conf，详见**附录**的附录G4。

7.4.2. 通过安装程序更新Dr.Web代理服务器

代理服务器配置文件

版本10或更低版本代理服务器配置文件：

文件	描述
drwcsd-proxy.xml	代理服务器配置文件（见**附录**中的附录G4）

版本11或更高版本代理服务器配置文件：

文件	描述
drwcsd-proxy.conf	代理服务器配置文件（见**附录**中的附录G4）
drwcsd-proxy.auth	访问Dr.Web服务器的身份认证数据（ID和密码）
drwcsd-proxy-trusted.list	Dr.Web服务器可信任证书列表
drwcsd-proxy-signed.list	代理服务器签名证书列表
drwcsd-proxy.pri	代理服务器加密私钥

OS Windows代理服务器的更新

利用安装程序自动更新。

从版本10或更低版本更新代理服务器的操作

1. 启动代理服务器程序文件。
2. 打开已安装有代理服务器软件上一版本的通知窗口，同时建议更新至新版本。删除老版本并安装新版本需点击**Upgrade**按钮。
3. 打开产品信息窗口。点击**Next**。
4. 在以下步骤对代理服务器进行的设置，与使用上一版本配置文件安装Dr.Web代理服务器相同。安装程序自动确定代理服务器安装目录、上次安装的配置文件的位置。如需可更改安装程序从自动搜索到的文件提取的设置。
5. 开始安装代理服务器版本12.0需点击**Install**按钮。

从版本11或更高版本更新代理服务器的操作

1. 启动代理服务器程序文件。

2. 打开已安装有代理服务器软件上一版本的通知窗口，同时建议更新至新版本。开始设置更新进程需点击**Upgrade**按钮。
3. 打开删除老版本代理服务器的信息窗口。开始删除需点击**Uninstall**。
4. 删除代理服务器老版本后开始安装新版本。打开产品信息窗口。点击**Next**。
5. 在以下步骤对代理服务器进行的设置，与使用上一版本配置文件安装Dr.Web代理服务器相同。安装程序自动确定代理服务器安装目录、上次安装的配置文件的位置。如需可更改安装程序从自动搜索到的文件提取的设置。
6. 开始安装代理服务器版本12.0需点击**Install**按钮。

OS UNIX代理服务器的安装

从版本11.0或更低版本更新代理服务器的操作



更新代理服务器时会删除配置文件配置文件 。必要时在更新代理服务器前请手动保存配置文件。

1. 开始更新请启动代理服务器程序文件：
   `./<软件版本>.tar.gz.run`
2. 完成更新后如需可将更新前保存的配置文件手动写入新配置文件。

从版本11.0.1更新代理服务器的操作

1. 开始更新请启动代理服务器程序文件：
   `./<软件版本>.tar.gz.run`
2. 删除老版本过程中会自动保存代理服务器配置文件。
3. 更新过程中会提示使用之前安装的代理服务器的配置文件备份：
   - 使用默认保存在`/var/tmp/drwcsd-proxy`目录的备份需点击ENTER。
   - 使用保存于另一目录的备份需手动输入备份路径。
   - 还可以不使用之前安装的代理服务器的配置文件，而是以默认设置安装代理服务器，操作是点击0。

索引

A

Active Directory
- 代理端安装 60
- 概述 35
- 删除代理端 74

D

Dr.Web服务器
- 安装，OS UNIX 42
- 安装，OS Windows 37
- 更新，OS UNIX 82
- 更新，OS Windows 77
- 卸载，OS UNIX 71
- 卸载，OS Windows 71

Dr.Web服务器发现服务 27

N

NAP Validator
- 安装 63

S

SRV协议 27

[其它]

安装 43
- NAP Validator 63
- 代理端 43
- 代理服务器 64
- 反病毒软件包 43
- 服务器，OS UNIX 42
- 服务器，OS Windows 37

安装包
- 个人 44, 47
- 类型,对比 46
- 组 44
- 组安装包 50
- 组成 44

安装程序
- 安装 50
- 类型 44
- 卸载 73
- 组成 44

安装页面 44

产品 20

创建
- 帐户，工作站 47
- 账户，代理服务器 64

代理端
- 安装 43, 50
- 安装，Active Directory 60
- 安装，本地 46
- 安装，远程 53, 56, 60
- 更新 88
- 删除，Active Directory 74
- 卸载，OS Windows 72

代理端安装 43
- Active Directory 60
- 安装程序 50
- 本地 46
- 个人安装包 47
- 远程 53, 56, 60
- 组安装包 50

代理服务器
- 安装 64
- 连接Dr.Web服务器 69
- 卸载 74
- 账户 64

反病毒软件包
- 安装 43
- 卸载 72

反病毒网络
- 创建 23

个人安装包
- 安装 47
- 概述 44

更新
- 代理端 88
- 服务器，OS UNIX 82
- 服务器，OS Windows 77

工作站
- 帐户，创建 47

公钥 32

加密
- 概述 28

流量
- 加密 28
- 压缩 28

流量压缩 28

密钥
- 加密 32
- 试用 22

索引

密钥
    授权密钥 22
删除代理端
    Active Directory 74
    OS Windows 72
    安装程序 73
试用密钥 22
授权 22
授权密钥
    获取 22
私钥 32
图标
    网络搜索仪 57
网络搜索仪 56
系统要求 16
卸载
    代理端 72
    代理服务器 74
    反病毒软件包 72
    服务器, OS UNIX 71
    服务器, OS Windows 71
    组件 72
账户
    代理服务器 64
    工作站 47
证书 32
注册
    Dr.Web产品 22
组安装包
    安装 50
    概述 44

© Doctor Web, 2021