EMAIL SECURITY MANAGER 帮助

Websense® Email Security Gateway

v7.8.x

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

R0527783

2014 年 5 月出版
美国和爱尔兰印制。

本文档所述的产品和 / 或使用方法受美国专利号 6,606,659 和 6,947,985 及其它正在申请的专利保护。

商标

Websense、Websense 徽标、Threatseeker 和 TRITON 是 Websense, Inc. 在美国和 / 或其它国家或地区的注册商标。Websense 在美国和国际市场还有许多其它未注册商标。所有其它商标归其各自所有者所有。

本产品包括:

ANTLR

如果满足以下条件，便允许以源代码和二进制形式再分发和使用（包含或不含修改）:

- 源代码的再分发必须保留以上版权通告、本条件列表及以下免责声明。
- 二进制形式的再分发必须在分发所提供的文档和 / 或其他材料中复制以上版权通知、本条件列表及以下免责声明。
- 事先未获特定的书面同意，作者或其责任者的名称不得用于认可或宣传本软件派生的产品。

本软件由版权持有人及责任者“按原样”提供，不含任何明确或隐含的保证，包括但不限于对适销性和特定用途适用性的隐含保证。对于因使用本软件而引起的任何形式的直接、间接、偶发、特殊、典型或随发损坏（包括但不限于替代品或服务的采购；使用、数据或利润损失；或业务中断），无论基于任何原因或任何责任理论，例如合同、严格责任或民事侵权（包括疏忽等），版权所有人或责任者概不负责，即使他们已被告知存在此类损害的可能性也一样。

Apache Software License 第 2 版

根据 Apache License 2.0 版（“许可证”）许可；只能根据许可证使用本文件。

在 http://www.apache.org/licenses/LICENSE-2.0 上可获取许可证副本。

只有在相关法律要求或书面同意后，才可“按原样”根据许可证分发软件，而不含任何明确或隐含的保证或条件。

有关根据许可证管理权限和限制的特定语言，请参阅许可证。

CKEditor for Java

根据 GNU 通用公共许可证 (GPL) 第 3 版（2007 年 6 月）许可。

前言

GNU 通用公共许可证是一种针对软件和其他种类作品的公共版权免费许可证。

大多数软件和其他实用性作品的许可证设计为禁止共享和更改。相反，GNU 通用公共许可证将保证您享有共享和更改所有版本之程序的自由 - 确保所有用户能够始终自由使用软件。我们，即 Free Software Foundation, 将 GNU 通用公共许可证用于我们的大多数软件；它还适用于其作者以此方式发布的任何其他作品。您也可以将其应用于您的计划。

我们谈到自由软件 (free software) 时，是指使用的自由，而不是价格的免费。我们的通用公共许可证设计为确保您：自由分发自由软件的副本（您也可针对它们收费）；根据需要获取源代码；更改软件或在新的免费计划中使用其组件；知道自己可以执行这些操作。

为保护您的权利，我们需要禁止他人拒绝您享有这些权利，或者要求您放弃这些权利。因此，如果您分发此软件的副本或者进行修改，也要肩负起尊重他人自由的责任。

例如，如果您分发此类程序的副本，无论是免费还是收费，都必须把您获得的自由同样地授予接收者。您必须确保他们也获得源代码，还必须向他们展示这些条款，确保他们知道自己享有这些权利。

使用 GNU GPL 的开发者通过两个步骤保护您的权利：(1) 声明软件的版权，以及 (2) 提供本许可证，授予您复制、分发和 / 或修改软件的合法权限。

为保护开发者和作者，GPL 明确阐释本自由软件不含任何保证。为了用户和作者的利益，GPL 要求修改过的版本必须标记为已更改，以免它们的问题被错误地归咎于先前版本的作者。

某些设备被设计为拒绝用户安装或运行其内部软件的修改版本，尽管制造商可以安装和运行它们。这从根本上违背了保护用户自由更改软件的理念。此类系统的滥用模式出现在个人所用的产品领域，这正是最让人无法接受的。因此，我们设计了此版本的 GPL 来禁止针对这些产品的上述做法。如果此类问题在其他领域大量涌现，我们已准备好在将来的 GPL 版本中根据需要扩展这项规定，以保护用户的自由。

最后，每个程序都不断地受到软件专利的威胁。政府不应该允许专利权限制通用计算机软件的开发和使用，但是在确实允许这种情况的地区，我们希望避免一种特殊的危险，即适用于自由程序的专利权可使程序有效私有化。为了防止这种情况，GPL 保证专利权无法让自由程序非自由化。

下面列出关于复制、分发和修改的具体条款和条件。

条款和条件

0. 定义。

“本许可证”指 GNU 通用公共许可证第 3 版。

“版权”还指适用于其他作品（如半导体防护罩）的版权保护法律。

“程序”指任何在本许可证下许可的受版权保护的作品。每个被许可方都称为“您”。“被许可方”和“接收者”可以是个人或组织。

“修改”作品指在需要获得版权许可的情况下，复制或改写作品的全部或一部分，这不同于完整的复制。最终作品被称为先前作品的“修改版本”或“基于”先前作品的作品。

“涵盖作品”指未经修改的程序或基于本程序的作品。

“传播”作品指在没有获得许可的情况下使用作品，根据适用的版权法这样做需要直接或间接承担侵权责任，不包括在计算机上执行程序或者修改私有副本。传播包括复制、分发（无论修改与否）、公开，以及在某些国家 / 地区的其他行为。

“转让”作品指任何使其他方能够制作或接收副本的传播方式。仅仅通过计算机网络和用户交互，而未涉及副本的传送，就不构成转让。

一个显示“适当法律通告”(Appropriate Legal Notices) 的交互用户界面应包含一项方便且突出的功能：(1) 显示适当的版权通告；(2) 告诉用户对该作品不负任何担保责任（除非提供了担保），被许可方可以根据本许可证转让该作品，以及如何查看本许可证的副本。如果此界面显示一个用户命令或选项列表（例如菜单），该列表中的重要项目就符合这一条件。

1. 源代码。

作品的“源代码”指作品便于修改的形式。“目标代码”指作品的任何非源代码形式。

“标准接口”有两种含义：一是由公认的标准机构定义的官方标准接口；二是针对某种特定编程语言指定的众多接口中，以该语言工作的开发者广泛使用的接口。

可执行作品的“系统函数库”不是指整个作品，而是包括同时符合以下两个条件的任何内容：(a) 包含在主要组件的正常包装中，但并不属于该主要组件；(b) 仅用于使作品能与该主要组件一起使用，或者用于实施已有公开源代码的标准接口。在此上下文中，“主要组件”指运行可执行作品的特定操作系统（如果有）的主要关键组件（内核、窗口系统等），或者用于生成该作品的编译器，或者用于运行该作品的目标代码解释器。

目标代码形式作品的“对应源代码”指生成、安装和（对可执行作品而言）运行该目标代码以及修改该作品所需的所有源代码，包括用于控制这些活动的脚本。但是，它不包括作品的系统库、通用工具，或在未经修改的情况下，完成这些活动所需的、并非作品一部分的常用免费程序。例如，对应源代码包括与作品的源文件相关联的接口定义文件，以及作品特定所需的共享库和动态链接子程序的源代码（例如因为这些子程序与该作品其他部分之间存在密切数据通信或控制流）。

对应源代码不需要包含用户可以从对应源代码的其他部分自动再生的任何内容。

对于源代码形式的作品而言，其对应源代码就是作品本身。

2. 基本许可。

所有根据本许可证授予的权利都是针对程序的版权有效期授予的，并且只要所述的条件得到满足，这些权利不可撤销。本许可证明确申明，您可以不受任何限制地运行未经修改的程序。对于运行涵盖作品时获得的结果，仅当该结果的内容构成涵盖作品时，才受本许可证约束。本许可证承认版权法赋予您正当使用权或其他同等的权利。

只要您的许可证仍然有效，您可以无条件地制作、运行和传播您未转让的涵盖作品。如果只是需要他人专为您修改涵盖的作品或向您提供运行这些作品的工具，则您可以向他人转让涵盖作品，只要您遵守本许可证中关于转让您不具有版权的所有材料的条款。因此，为您制作或运行涵盖作品的人必须仅代表您且在您的指示和控制下做到这些，并禁止他们在与您的关系以外制作任何您拥有版权的资料的副本。

仅当下述条件得到满足时，允许在任何其他情况下进行转让。再许可是不被允许的，第 10 条使其变得没有必要。

3. 保护用户的法律权利不受反规避法侵犯。

在任何履行 1996 年 12 月 20 日通过的《世界知识产权组织版权条约》(WIPO) 第 11 章中所述义务的适用法律，或者禁止或限制这种规避方法的类似法律下，涵盖作品都不会被认定为有效技术措施的一部分。

当您转让涵盖作品时，您将放弃任何禁止技术措施规避行为的法律权利，条件是这些规避行为是在对该作品行使本许可证中的权利时进行的；您亦放弃任何限制操作或修改该作品以执行作品用户、您或第三方禁止技术措施规避行为的法律权利的意图。

4. 转让完整副本。

您可以通过任何媒介按原样转让程序源代码的完整副本，但必须在每个副本明显且适当的位置附上适当的版权通告；照搬声明本许可证以及按照第 7 条添加的任何非许可条款适用于该代码的所有通告；照搬表示不含任何保证的所有通告；向所有接收者随程序提供本许可证副本。

您可以针对转让的每个副本收取或不收取任何费用，也可以有偿提供支持或保证。

5. 转让修改过的源代码版本。

您可以根据第 4 条的条款以源代码形式转让基于程序的作品或用于从程序制作该作品的修改，但必须同时满足下列条件:

a) 作品必须包含明确的通告说明您已修改它，并注明相关日期。

b) 作品必须包含明确的通告，说明其根据本许可证以及第 7 条添加的任何条件发布。这条要求修改了第 4 条的“照搬所有通告”的要求。

c) 您必须根据本许可证将整个作品作为一个整体许可给任何获得副本的人。因此，本许可证将同任何按照第 7 条添加的条款一起应用于整个作品及其所有部分，无论它们是以什么形式打包。本许可证不允许以其他任何形式许可该作品，但如果您在个别情况下收到任何权限，本许可证并不否定此类权限。

d) 如果作品包含交互用户界面，每个界面必须显示适当的法律通告；但是，如果程序包含未显示适当法律通告的交互界面，您的作品无需让它们显示。

如果将一个涵盖作品与其他本身不是该涵盖作品的扩展的单独作品联合在一起，而联合的目的不是为了在存储或分发介质上生成更大的程序，且此联合体及其产生的版权没有用来限制单个作品允许的联合程序用户的访问或法律权利，这样的联合体就称为“聚集体”。在聚集体中包含涵盖作品并不会使本许可证应用于该聚集体的其他部分。

6. 转让非源代码形式的副本。

您可以根据第 4 和第 5 条条款以目标代码形式转让涵盖作品，但同时必须以以下一种方式根据本许可证条款转让机器可读的对应源代码:

a) 在实体产品（包括实体分发介质）中或作为其一部分转让目标代码，并在常用于软件交换的耐用实体介质上转让对应源代码。

b) 在实体产品（包括实体分发介质）中或作为其一部分转让目标代码，并随附有效期至少三年且长度与您为该产品模型提供配件或客户支持相等的书面报价，向任何拥有该目标代码的人 (1) 在常用于软件交换的耐用实体介质上，以不高于您实际执行此源代码转让的合理成本的价格，提供本许可证涵盖产品中所有软件的对应源代码的副本；或者 (2) 免费提供从网络服务器复制对应源代码的权限。

c) 转让目标代码的单独副本，并随附提供对应源代码的书面报价的副本。此行为仅允许偶尔发生且不能盈利，并且仅在您根据第 6b 小节随此类报价收到目标代码时才适用。

d) 通过提供对指定位置的访问权限（免费或收费）转让目标代码，并在不增加费用的情况下提供从同一位置以相同方式访问对应源代码的同等权限。您无需要求接收者随目标代码一起复制对应源代码。如果复制目标代码的位置是网络服务器，对应源代码可以在其他支持相同复制工具的服务器上（由您或第三方操作），但您必须在目标代码旁边明确指出在何处可以找到对应源代码。无论由哪个服务器托管对应源代码，您都有义务确保它在任何有需要的时候都可用，从而满足这些要求。

e) 使用点对点传输转让目标代码，但您需要告知他人在何处根据第 6d 小节免费向公众提供了作品的目标代码和对应源代码。

在转让目标代码作品时，不需要包含目标代码中可分离的部分，该部分的源代码作为系统函数库排除在对应源代码之外。

“用户产品”指 (1)“消费品”，即通常用于个人、家人或家庭目的的任何有形个人财产；或者 (2) 任何针对家居生活设计或销售的东西。如果在确定一个产品是否为消费品时存有疑问，应以有利于覆盖面的结果加以判断。对于特定用户接收到的特定产品，“正常使用”指按照典型或通常方法使用该类产品，无论该特定用户的身份、其实际使用的方式或该产品要求的使用方式如何。一个产品是否为消费品与该产品是否具有实质性的商业、工业或非消费类用途无关，除非此类用途代表该产品唯一的重要使用模式。

用户产品的“安装信息”指从其对应源代码的修改版本安装和执行该用户产品中涵盖作品的修改版本所需要的任何方法、步骤、授权密钥或其他信息。这些信息必须足以确保修改后的目标代码绝不会仅仅因为被修改过而不能运行或正常运行。

如果您根据本条款转让用户产品中包含的、其随附的或者专用于其中的任何目标代码作品，并且用户产品的所有权和使用权都永久地或在固定期间内转让给接收者（无论此交易的特点如何），根据本条款转让的对应源代码必须随附安装信息。但是如果您或者任何第三方都没有保留在用户产品上安装修改过的目标代码的能力（例如作品安装在了 ROM 上），那么这项要求不适用。

提供安装信息的要求并不包括为接收者修改或安装的作品或者修改或安装该作品的用户产品，继续提供支持服务、担保或更新。当修改本身实质上对网络运行产生了负面影响或者违反了网络通信的规则和协议时，网络访问可能被拒绝。

根据本条款转让的对应源代码和提供的安装信息必须采用公共记录的格式（并随附一个以源代码形式提供给公众的实现方法），且不能要求任何用于解压缩、阅读或复制的特殊密码或密钥。

7. 附加条款。

“附加许可”条款规定本许可证中一个或多个条件的例外情况，是本许可证条款的补充。只要对整个程序都适用的附加许可在适用法律下有效，它们就应当被视为本许可证的内容。如果附加许可仅适用于程序的一部分，那么可单独根据这些许可来使用该部分，但整个程序仍然受本许可证的管辖，而不管附加许可如何。

当您转让涵盖作品的副本时，可以选择删除该副本或副本任何部分的任何附加许可。（当您修改作品时，可编写附加权限以要求在某些情况下将其自身删除。）您可以将附加权限放在材料里，添加到您拥有或可授予适当版权许可的涵盖作品中。

尽管有本许可证中的任何其他规定，对于您添加到涵盖作品的材料，您都可以（如果获得该材料版权持有人的授权）使用以下条款补充本许可证:

a) 拒绝担保或者以与本许可证第 15 和第 16 条条款不同的方式限制责任；或者

b) 要求在该材料中或包含该材料的作品显示的适当法律通告中保留指定的合理法律通告或作者归属；或者

c) 禁止误传该材料的来源，或者要求以合理的方式将该材料的修改版本标记为与原始版本不同的版本；或者

d) 限制以宣传为目的使用该材料的许可方名称或作者姓名；或者

e) 拒绝根据商标法授予使用一些商号、商标或服务标记的权利；或者

f) 要求任何转让该材料（或其修改版本）的人使用对接收者的契约性责任假设对该材料的许可方和作者进行保护，避免这些契约性假设直接造成许可方和作者的责任。

所有其他非许可附加条款都被视为第 10 条规定的“进一步限制”。如果您收到的程序或其任何部分包含声明其受本许可证管辖的通告，并附有进一步限制条款，那么您可以删除该条款。如果许可文档包含进一步限制，但是允许根据本许可证再许可或转让，只要此进一步限制在此类再许可或转让中无法保留下来，您就可以在涵盖作品中添加该许可文档条款管辖的材料。

如果您根据本条款向涵盖作品添加条款，则必须在相关的源代码文件中加入一条适用于这些文件的附加条款的声明，或者一个指明在何处可以找到适用条款的通告。

附加条款（无论是许可还是非许可）可以写在一个单独的书面许可中，也可以声明为例外情况；这两种方法都可以实现上述要求。

8. 终止。

除本许可证明确规定之外，不能传播或修改涵盖作品。以其他任何方式尝试传播或修改涵盖作品都是无效的，将会自动终止您在此许可证下获得的权利（包括根据第 11 条的第三段授予的任何专利许可）。

但是，如果您停止所有违反本许可证的行为，您从特定版权持有人处获取的许可证可通过以下方式恢复：(a) 暂时地拥有许可证，直到版权持有人明确地终止许可；(b) 如果在您停止违反行为后的 60 天内，版权持有人没有以某种合理的方式通知您的违反行为，那么您可以永久地获取本许可证。

此外，如果特定版权所有人以某种合理的方式通知您的违反行为，而这是您第一次收到来自该版权持有人的许可证违反通知（对于任何作品），并在收到通知后的 30 天内改正了违反行为，那么您从该版权持有人处获取的许可证将永久地恢复。

当您的权利根据本条款被终止时，从您那里获取副本或权利的各方只要保持不违反本许可证，其许可就不会被终止。如果您的权利被终止且未得到永久恢复，将没有资格根据第 10 条获取相同材料的新许可证。

9. 获取副本不需要接受本许可证。

您不需要为了接收或运行程序的副本而接受本许可证。仅仅是因为使用点对点传输接收副本而导致涵盖作品的传播，也不要求您接受本许可证。但是，除了本许可证外，任何许可证都不能授予您传播或修改涵盖作品的权限。如果您不接受本许可证，这些操作会侵犯版权。因此，只要修改或传播涵盖作品，则表示您接受本许可证。

10. 下游接收者的自动许可。

每次转让涵盖作品时，接收者都会自动从原始许可方处收到许可证，许可其根据本许可证运行、修改和传播该作品。您没有强制第三方履行本许可证的义务。

“实体交易”指转移组织的控制权或全部资产、拆分组织或者合并组织的交易。如果涵盖作品的传播是由实体交易导致的，该交易中接收作品副本的各方都还将收到其之前的所有者拥有或者可根据前面条款提供的任何许可证，以及从其之前的所有者处获取作品的对应源代码的权利，只要之前的所有者拥有或能够通过合理的努力获取这些源代码。

您不得对根据本许可证授予或申明的权利做任何其他限制。例如，您不可以因为他人行使本许可证授予的权利而向其收取许可费、版权费或其他费用，也不可以因为他人制作、使用、销售、许诺销售或进口程序或其任何部分而提起诉讼（包括交叉诉讼或反诉），声称其侵犯任何专利权。

11. 专利权。

“贡献者”指根据本许可证授权使用程序或程序所基于的作品的版权所有人。因此许可的作品被称为贡献者的“贡献者版本”。

贡献者的“实质专利权利要求”指该贡献者所拥有或控制的所有专利权利要求（无论是已获得的还是在将来获得的），其可能会受到某种方式的侵犯，且本许可证允许制作、使用或销售其贡献者版本，但不包括仅由于对贡献者版本进一步修改而受到侵犯的权利要求。就本定义而言，“控制”包括以与本许可证要求一致的方式授予专利再许可的权利。

每个贡献者根据该贡献者的实质专利权利要求授予您非专有、全球性、无版权费的专利许可证，允许您制作、使用、销售、许诺销售、进口及以其他方式运行、修改和传播其责任者版本的内容。

在以下三个段落中，“专利许可证”指不执行专利权的任何明示协议或承诺，无论有无特定名称（例如，行使专利权的明确许可，或者不因专利侵权而起诉的契约）。向一方“授予”此专利许可证指达成或做出此类不向该方提出执行专利权的协议或承诺。

如果您有意依赖专利许可证转让涵盖作品，而根据本许可证条款，该作品的对应源代码并不能通过网络服务器或其他有效途径免费供公众复制，您必须：(1) 使对应源代码可按上述方法访问；或者 (2) 放弃从该特定作品的专利许可证获取利益；或者 (3) 以某种与本许可证要求一致的方式使该专利许可证延伸至下游接收者。“有意依赖”指您实际知道除了获取专利许可证外，您在某个国家 / 地区转让涵盖作品或接收者对于涵盖作品的使用，会侵犯该国家 / 地区的一个或多个可确认的专利权，而您有理由相信这些专利权是有效的。

在依据或涉及单个交易或安排时，如果您通过获取涵盖作品的转让来进行转让或传播，并向接收该涵盖作品的某些组织授予专利许可证，以允许他们使用、传播、修改或转让该涵盖作品的特定副本，那么您授予的专利许可证将自动延伸至该涵盖作品及以其为基础的作品的所有接收者。

如果专利许可证不包含在其涵盖范围内、禁止行使一项或多项本许可证明确授予的权利，或者以不执行这些权利为条件，则它是“不公平的”。在以下情况下，您不可以转让涵盖作品：如果您与软件分发行业的第三方有协议，而该协议要求您根据该作品转让活动的规模向该第三方付费，同时该第三方根据协议向从您那里接收涵盖作品的任何方授予一份涉及以下内容的不公平专利许可证，(a) 涉及您转让的涵盖作品的副本（或从这些副本制作的副本）；或者 (b) 主要针对或涉及包含该涵盖作品的特定产品或联合体。如果您签署该协议或获得该专利许可证的日期早于 2007 年 3 月 28 日，那么您不受本条款约束。

本许可证中的任何内容均不应被解释为排除或限制任何暗示许可证，或其他在适用的专利法下以其他方式保护您的专利不受侵犯的措施。

12. 不要放弃他人的自由。

如果您遇到与本许可证的条件相冲突的情况（无论是法院命令、协议还是其他），您遵守本许可证条件的责任也不会被免除。如果您无法同时满足本许可证规定的义务和其他相关义务，那么其结果便是您不得转让涵盖作品。例如，如果您同意要求您向通过您获得程序的人收取再转让费的条款，则您满足这些条款及本许可证要求的唯一方式是完全禁止转让程序。

13. 与 GNU Affero 通用公共许可证一起使用。

尽管本许可证中有任何其他规定，您有权将任何涵盖作品与基于 GNU Affero 通用公共许可证第 3 版许可的作品进行链接或组合，以产生单个组合作品，并有权转让最终作品。本许可证的条款将继续适用于属于涵盖作品的部分，但是 GNU Affero 通用公共许可证中第 13 条关于通过网络交互的特殊要求将适用于整个组合。

14. 本许可证的修订版。

Free Software Foundation 可能随时发布修订和 / 或新增的 GNU 通用公共许可证版本。这些新版本的精神类似于现有版本，可能会更详细地说明新的问题。

每个版本都使用版本号加以区分。如果程序规定 GNU 通用公共许可证“或任何更新版本”采用特定版本号，您可以选择遵守 Free Software Foundation 发布的该版本或任何更新版本的条款及条件。如果程序未规定 GNU 通用公共许可证的版本号，您可以选择 Free Software Foundation 发布的任何版本。

如果程序规定能够由代理决定可使用 GNU 通用公共许可证的哪些将来版本，那么该代理接受任何版本的公开声明将会永久性地授权您为程序选择该版本。

更新的许可证版本可能会授予您其他或不同的权限。但是，您选择采用更新版本并不会对任何作者或版权持有人强加任何其他义务。

15. 保证免责声明。

在相关法律允许的范围 ，对程序不负任何保证责任。除非版权持有人和 / 或其他方另有书面规定，否则程序“按原样”提供，且不含任何明确或隐含的保证，包括但不限于适销性和特定用途适用性的隐含保证。关于程序质量和性能的全部风险由您自己承担。如果证明程序有缺陷，您自行承担所有必要服务、修复或纠正的费用。

16. 责任限制。

在任何情况下，除非相关法律要求或有书面协议，否则对于因使用程序或程序无法使用而引起的任何损害，包括任何一般、特殊、偶发或随发损害（包括但不限于数据泄露，或者造成您或第三方保留的数据不准确或

丢失，或者程序无法与其他程序协同运行），任何版权持有人或者可能按上述要求修改和 / 或转让的任何其他方概不负责，即使版权持有人或其他方已被告知存在此类损害的可能性也一样。

17. 第 15 和 16 条的解释。

如果上述保证免责声明和责任限制不能根据其条款获得当地法律效力，复审法院应采用最接近于完全放弃程序相关的所有民事责任的当地法律，除非责任保证或假设附有程序副本以收取费用。

条款和条件结束

dom4j

如果满足以下条件，便允许以源代码和二进制形式再分发和使用（包含或不含修改）：

- 源代码的再分发必须保留以上版权通告、本条件列表及以下免责声明。
- 二进制形式的再分发必须在分发所提供的文档和 / 或其他材料中复制以上版权通知、本条件列表及以下免责声明。
- 事先未获特定的书面同意，作者或其责任者的名称不得用于认可或宣传本软件派生的产品。

本软件由版权持有人及责任者“按原样”提供，不含任何明确或隐含的保证，包括但不限于对适销性和特定用途适用性的隐含保证。对于因使用本软件而引起的任何形式的直接、间接、偶发、特殊、典型或随发损坏（包括但不限于替代品或服务的采购；使用、数据或利润损失；或业务中断），无论基于任何原因或任何责任理论，例如合同、严格责任或民事侵权（包括疏忽等），版权所有人或责任者概不负责，即使他们已被告知存在此类损害的可能性也一样。

Bouncy Castle

特此授权任何人免费获取本软件及相关文档文件（“软件”）的副本，用以无限制地处理软件，包括但不限于使用、复制、修改、合并、发布、分发、再许可和 / 或出售软件副本的权利，以及允许获得软件的个人按照下列条件执行这些操作:

在软件的所有副本或主体部分应包含上述版权通知及本许可通告。

软件“按原样”提供，不含任何形式的明确或隐含保证，包括但不限于适销性、特定用途适用性和非侵权的保证。在任何情况下，对于因软件、软件的使用或其他处理而引起或与之相关的任何索赔、损害或其他责任，无论是否基于合同或侵权行为，作者或版权持有人概不负责。

Free Software Foundation, Inc.

GNU 通用公共许可证

第 2 版，1991 年 6 月

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

每个人都可以按原样复制和分发本许可文档的副本，但不允许做任何更改。

前言

大多数软件的许可证设计为禁止共享和更改。相反，GNU 通用公共许可证将保证您享有共享和更改自由软件的自由 - 确保所有用户都自由使用软件。这个通用公共许可证适用于 Free Software Foundation 的大多数软件及其作者承诺使用它的任何其他计划。（某些其它的 Free Software Foundation 软件不在 GNU Lesser 通用公共许可证的范围内。）您也可以将其应用于您的计划。

我们谈到自由软件 (free software) 时，是指使用的自由，而不是价格的免费。我们的通用公共许可证设计为确保您: 自由分发自由软件的副本（您也可针对此服务收费）；根据需要获取源代码；更改软件或在新的免费计划中使用其组件；知道自己可以执行这些操作。

为保护您的权利，我们需要实施一些限制，禁止任何人拒绝您享有这些权利，或者要求您放弃这些权利。这些限制会转化为您在分发或修改软件副本时应承担的特定责任。

例如，如果您分发此类程序的副本，无论是免费还是收费，都必须向接收者授予您拥有的所有权利。您必须确保他们也获得源代码，还必须向他们展示这些条款，确保他们知道自己享有这些权利。

我们通过两个步骤保护您的权利：(1) 为软件加入版权保护，以及 (2) 提供本许可证，授予您复制、分发和 / 或修改软件的合法权限。

此外，为保护每个作者以及我们的权益，我们要确定每个人都了解，本自由软件不含任何保证。如果软件被其他人修改并传递，希望接收者了解其并非原版软件，由此造成的任何问题都不会影响原作者的声誉。

最后，任何免费程序都不断地受到软件专利的威胁。我们希望不要让免费软件的再分发者个人获取专利许可证，而避免使程序从实质上变为专有软件。为了防范这种情况，我们明确表示，任何专利都必须许可每个人免费使用，或者根本不需要许可。

下面列出关于复制、分发和修改的具体条款和条件。

关于复制、分发和修改的条款及条件

0. 对于任何程序或其他作品，如果版权持有人在其中插入了通告，表示可根据此通用公共许可证的条款分发，则适用于本许可。下面提到的“程序”指的是任何这样的程序或作品；而“基于程序的作品”指的是程序或者任何受版权法约束的衍生作品：也就是说，包含程序或其部分内容的作品可以按原样复制或者修改及 / 或翻译成其他语言。（在下文中，术语“修改”包括但不限于翻译行为。）每个被许可方都称为“您”。

复制、分发和修改以外的其他活动超出了本许可证的范围。运行程序的行为不受限制，程序的输出仅在其内容构成基于程序的作品（独立于运行程序的结果）时才属于许可证范围。是否符合此条件要视程序的运行结果而定。

1. 您可以在任何介质中按原样复制和分发程序源代码的副本，但必须在每个副本明显且适当的位置发布版权通告和保证免责声明；照搬所有引用本许可证以及表示不含任何保证的所有通告；向程序的任何其他接收者随程序提供本许可证副本。

您可以针对传输副本的实际行为收费，也可以选择收费提供保证。

2. 您可以修改程序的副本或其任何部分，从而在程序的基础上形成作品，然后根据上述第 1 条的条款复制和修改此类修改或作品，但同时必须满足下列条件:

a) 修改后的文件必须在显要位置列出通告表示您已更改文件，并列出更改日期。

b) 全部或部分或者派生自程序或其任何部分的任何作品在分发或发布时，必须根据本许可证的条款整体免费许可给所有第三方。

c) 如果修改后的程序在运行时以交互方式正常显示命令，您必须使其在以最普通的方式交互式运行时，印出或显示出公告，包括适当的版权通告以及表示不含保证（或者表示您提供保证）的通告，并说明用户可以根据这些条件再分发程序，同时告诉用户如何查看此许可证的副本。（例外：如果程序本身是交互式的，但不能正常印出此类公告，则您在程序基础上创建的作品不需要印出公告。）

这些要求整个适用于修改的作品。如果该作品可识别的部分并非派生自程序，并且可以合理认为其本身为独立的作品，则在您将其作为单独的作品分发时，此许可证及其条款不适用于这些部分。但是，如果您分发的部分是作为基于程序的作品整体的一部分，则整体分发必须遵守此许可证的条款，其对于其他许可证的权限延伸到整个作品，进而延伸到每个部分（不管作者是谁）。

因此，本条款的目的不是要求权利或同意完全由您自己编写作品的权利，而是行使控制分发程序派生品或以程序为基础的集体作品的权利。

此外，基于程序的其他作品与程序（或基于程序的作品）在存储或分发介质的卷中合并，并不会使其他作品进入此许可证的范围。

3. 您可以根据上述第 1 和第 2 条的条款以对象代码或可执行文件形式复制和分发程序（或第 2 条下基于程序的作品），但同时必须执行下列操作之一:

a) 随附完整的对应机器可读源代码，必须根据上述第 1 和第 2 条的条款在常用于软件交换的介质上分发；或者

b) 随附至少三年有效的书面报价，向任何第三方提供对应源代码的完整机器可读副本（收费不能超过您实际执行源代码分发的成本），以根据上述第 1 和第 2 条的条款在常用于软件交换的介质上分发；或者

c) 将您收到的信息按原样随附到用以分发对应源代码的报价中。（此方式仅适用于非商业开发，并且仅在您根据上面 b 小节随此类报价收到对象代码或可执行文件形式的程序时才适用。）

作品的源代码是指作品便于修改的形式。对于可执行程序，完整的源代码是指其包含的所有模块的所有源代码，加上相关的界面定义文件，以及用于控制可执行程序编译和安装的脚本。但有一个特殊的例外，分发的源代码不需要包含通常随承载可执行程序的操作系统主要组件（编译器、核心等）分发（以源代码或二进制形式）的任何内容，除非组件本身附有可执行程序。

如果分发可执行程序或对象代码的方式是让人访问目的地的副本，则提供从同一地方复制源代码的同等访问权限也被视为分发源代码，即使没有强迫第三方随对象代码复制源代码也一样。

4. 除了本许可证明确规定的之外，不得复制、修改、再许可或分发程序。以其他任何方式尝试复制、修改、再许可或分发程序都是无效的，将会自动终止您在此许可证下的权利。但是，在此许可证下收到副本或获得权利的任何方，只要完全遵守许可证的条款，其许可证不会被终止。

5. 您不必接受此许可，因为您没有签署。但是，没有人授予您修改或分发程序或其派生作品的权限。如果您不接受此许可证，法律禁止您执行这些操作。因此，只要修改或分发程序（或基于程序的任何作品），则表示您接受此许可证及其关于复制、分发或修改程序或其派生作品的所有条款。

6. 每次再分发程序（或基于程序的任何作品）时，接收者会自动收到原始许可人的许可证，许可其根据这些条款及条件复制、分发或修改程序。您不得对接收者行使许可证授予的权利做任何其他限制。对于第三方是否遵守此许可证，您不承担任何责任。

7. 如果因法院判决、专利侵权指控或任何其他原因（不限于专利问题）导致您的情况（无论是法院命令、协议还是其他）与此许可证的条件相冲突，不会免除您遵守此许可证条件的责任。如果您无法同时履行此许可证规定的责任及任何其他相关责任，则不得分发程序。例如，如果专利许可证不允许所有直接或间接通过您获得副本的人免费再分发程序，则您满足此规定及此许可证要求的唯一方式是完全禁止分发程序。

如果本条款的任何部分在特定环境下无效或不可实施，则其余部分仍然适用，并且在其他环境下本条款全部适用。

本条款的目的并非诱使您侵犯任何专利或其他专有权利或抗辩此类权利要求的有效性，其唯一目的是按照公共许可证实践保护自由软件分发系统的完整性。得益于系统的持续应用，许多人对通过该系统分发的各类软件做出了重大的贡献；作者 / 供稿者有权决定其是否愿意通过任何其他系统分发软件，被许可人对此没有选择权。

本条款旨在彻底明确此许可证其余部分的重要性。

8. 如果程序的分发和 / 或使用因专利或有版权的接口而被限于在特定国家使用，则根据此许可证发布程序的原始版权持有人可加入明确的地区分发限制要求，排除这些国家，只允许在未排除的国家内或国家之间分发。在这种情况下，此许可证会合并该限制，就像这些限制写在此许可证的正文中一样。

9. Free Software Foundation 可能随时发布修订和 / 新增的通用公共许可证版本。这些新版本的精神类似于现有版本，可能会更详细地说明新的问题。

每个版本都使用版本号加以区分。如果程序规定本许可证及“任何更新版本”采用的版本号，您可以选择遵守 Free Software Foundation 发布的该版本或任何更新版本的条款及条件。如果程序未规定此许可证的版本号，您可以选择 Free Software Foundation 发布的任何版本。

10. 如果要将程序的部分内容合并到分发条件不同的其他免费程序中，请写信给作者以获得允许。对于 Free Software Foundation 发布的有版权保护的软件，请写信给 Free Software Foundation ；我们有时会有例外规定。我们的决定遵循两个目标：维持我们自由软件所有派生作品的自由状态；提倡以一般方式共享和重复使用软件。

不含保证

11. 由于程序是免费许可的，因此在相关法律允许的范围内不含任何保证。除非版权持有人和 / 或其他方另有书面规定，否则程序“按原样”提供，且不含任何明确或隐含的保证，包括但不限于适销性和特定用途适用性的隐含保证。关于程序质量和性能的全部风险由您自己承担。如果证明程序有缺陷，您自行承担所有必要服务、修复或纠正的费用。

12. 在任何情况下，除非相关法律要求或有书面协议，否则对于因使用程序或程序无法使用而引起的任何损害，包括任何一般、特殊、偶发或随发损害（包括但不限于数据泄露，或者造成您或第三方保留的数据不准确或丢失，或者程序无法与其他程序协同运行），任何版权持有人或者按上述要求修改和 / 或再分发程序的任何其他方概不负责，即使版权持有人或其他方已被告知存在此类损害的可能性也一样。

Libevent

版权所有 (c) 2000-2007 Niels Provos <provos@citi.umich.edu> 。保留所有权利。

如果满足以下条件，便允许以源代码和二进制形式再分发和使用（包含或不含修改）：

- 源代码的再分发必须保留以上版权通告、本条件列表及以下免责声明。
- 二进制形式的再分发必须在分发所提供的文档和 / 或其他材料中复制以上版权通知、本条件列表及以下免责声明。
- 事先未获特定的书面同意，作者或其责任者的名称不得用于认可或宣传本软件派生的产品。

本软件由版权持有人及责任者“按原样”提供，不含任何明确或隐含的保证，包括但不限于对适销性和特定用途适用性的隐含保证。对于因使用本软件而引起的任何形式的直接、间接、偶发、特殊、典型或随发损坏（包括但不限于替代品或服务的采购；使用、数据或利润损失；或业务中断），无论基于任何原因或任何责任理论，例如合同、严格责任或民事侵权（包括疏忽等），版权所有人或责任者概不负责，即使他们已被告知存在此类损害的可能性也一样。

net

版权所有 © 1998 - 2004 Mike D. Schiffman

保留所有权利。

如果满足以下条件，便允许以源代码和二进制形式再分发和使用（包含或不含修改）：

- 源代码的再分发必须保留以上版权通告、本条件列表及以下免责声明。
- 二进制形式的再分发必须在分发所提供的文档和 / 或其他材料中复制以上版权通知、本条件列表及以下免责声明。
- 事先未获特定的书面同意，< 组织 > 或其责任者的名称不得用于认可或宣传本软件派生的产品。

本软件由版权持有人及责任者“按原样”提供，不含任何明确或隐含的保证，包括但不限于对适销性和特定用途适用性的隐含保证。对于因使用本软件而引起的任何形式的直接、间接、偶发、特殊、典型或随发损害（包括但不限于替代品或服务的采购；使用、数据或利润损失；或业务中断），无论基于任何原因或任何责任理论，例如合同、严格责任或民事侵权（包括疏忽等），< 版权持有人 > 概不负责，即使他们已被告知存在此类损害的可能性也一样。

Net-SNMP

如果满足以下条件，便允许以源代码和二进制形式再分发和使用（包含或不含修改）：

- 源代码的再分发必须保留以上版权通告、本条件列表及以下免责声明。
- 二进制形式的再分发必须在分发所提供的文档和 / 或其他材料中复制以上版权通知、本条件列表及以下免责声明。
- 事先未获特定的书面同意，作者或其责任者的名称不得用于认可或宣传本软件派生的产品。

本软件由版权持有人及责任者“按原样”提供，不含任何明确或隐含的保证，包括但不限于对适销性和特定用途适用性的隐含保证。对于因使用本软件而引起的任何形式的直接、间接、偶发、特殊、典型或随发损坏（包括但不限于替代品或服务的采购；使用、数据或利润损失；或业务中断），无论基于任何原因或任何责任理论，例如合同、严格责任或民事侵权（包括疏忽等），版权所有人或责任者概不负责，即使他们已被告知存在此类损害的可能性也一样。

nl

GNU LESSER 通用公共许可证

第 3 版，2007 年 6 月

每个人都可以按原样复制和分发本许可文档的副本，但不允许做任何更改。

此版本的 GNU Lesser 通用公共许可证包括 GNU 通用公共许可证第 3 版的条款和条件，并增补了下列其他权限。

0. 其他定义。

如本文所用，“本许可证”是指 GNU Lesser 通用公共许可证第 3 版，“GNU GPL”是指 GNU 通用公共许可证第 3 版。

“函数库”是指本许可证而非应用程序或组合作品（定义如下）管辖的涵盖作品。

“应用程序”是指任何利用函数库提供的接口的作品，但它不是基于函数库的。定义由函数库定义的类的子类被视为使用函数库提供的接口的模式。

“组合作品”是指通过将应用程序与函数库合并或链接而产生的作品。生成组合作品所使用的函数库特定版本也称为“链接版本”。

组合作品的“最小对应源代码”是指组合作品的对应源代码，不包括组合作品部分的任何源代码，被看作独立作品，是基于应用程序，而不是基于链接版本。

组合作品的“对应应用程序代码”是指应用程序的目标代码和 / 或源代码，包括从应用程序复制组合作品所需的任何数据和实用程序，但不包括组合作品的系统库。

1. GNU GPL 第 3 条例外。

可以根据本许可证第 3 和第 4 条转让涵盖的作品，不受 GNU GPL 第 3 条的约束。

2. 转让修改过的版本。

如果修改函数库的副本，并且在修改的版本中，有个工具用到使用该工具的应用程序提供的函数或数据，而不是调用此工具时传递的参数，则可以转让修改版本的副本:

a) 根据本许可证，您必须确保在应用程序不提供函数或数据时，该工具仍能工作且其执行的任何操作仍然有意义，或者

b) 根据 GNU GPL，本许可证没有适用于该副本的额外权限。

3. 目标代码合并来自函数库标题文件的材料。

应用程序的目标代码形式可以合并来自属于函数库的标题文件的材料。可以根据您选择的条款转让此类目标代码，前提是，如果合并的材料不限于数字参数、数据结构布局和存取器、小的宏、内联函数和模板（长度最多 10 行），则可以执行下列两项操作:

a) 在目标代码的每个副本显眼之处提供如下声明：此作品使用函数库，且函数库及其用途受本许可证的约束。

b) 为目标代码附上 GNU GPL 副本和本许可文档。

4. 组合作品。

您可以根据所选的条款转让组合作品，有效地不限制修改组合作品所含函数库的各部分，以及调试此类修改而进行的反向工程，前提是您还执行以下各项操作:

a) 在组合作品的每个副本显眼之处提供如下声明：此作品使用函数库，且函数库及其用途受本许可证的约束。

b) 为组合作品附上 GNU GPL 副本和本许可文档。

c) 对于在执行过程中会显示版权声明的组合作品，在这些声明中包含函数库版权声明，以及将用户指引到 GNU GPL 副本和本许可文档的参考信息。

d) 执行下列操作之一:

0) 根据本许可证的条款转让最小对应源代码和采用合适形式的对应应用程序代码，根据条款，允许用户重新将应用程序与链接版本的修改版本进行组合或链接，以便以 GNU GPL 第 6 条指定的转让对应源代码的方式生成修改的组合作品。

1) 使用合适的共享函数库机制与函数库链接。合适的机制应当：(a) 在运行时使用用户计算机系统上已存在的函数库副本；且 (b) 可与接口兼容链接版本的函数库的修改版本一起正确操作。

e) 提供安装信息，但前提是根据 GNU GPL 第 6 条您本来就需要提供此类信息，此类信息是安装和执行组合作品的修改版本所必需的，组合作品是通过重新将应用程序与链接版本的修改版本进行组合或链接而产生的。（如果使用选项 4d0，则安装信息必须包括最小对应源代码和对应应用程序代码。如果使用选项 4d1，则必须以 GNU GPL 第 6 条指定的转让对应源代码的方式提供安装信息。）

5. 组合函数库。

您可以将是基于函数库的作品的函数库工具和不是应用程序也不是本许可证所涵盖范围的其他函数库工具并排放在单个函数库中，并根据您选择的条款转让此类组合函数库，前提是执行下列两项操作:

a) 和合并的函数库一起附上基于本函数库的相同作品的副本（与任何其他函数库工具分开），并根据本许可证条款转让。

b) 在合并函数库的显眼之处提供如下声明：合并函数库的一部分是基于本函数库的作品；并说明在何处可以找到随附的相同作品的未合并形式。

6. GNU Lesser 通用公共许可证的修订版。

Free Software Foundation 可能随时发布修订和 / 或新增的 GNU Lesser 通用公共许可证版本。这些新版本的精神类似于现有版本，可能会更详细地说明新的问题。

每个版本都使用版本号加以区分。如果您收到的函数库规定 GNU Lesser 通用公共许可证“或任何更新版本”采用特定版本号，您可以选择遵守 Free Software Foundation 发布的该版本或任何更新版本的条款及条件。如果您收到的函数库未规定 GNU Lesser 通用公共许可证的版本号，您可以选择 Free Software Foundation 发布的任何版本。

如果您收到的函数库规定可由代理决定是否要应用 GNU Lesser 通用公共许可证的将来版本，那么该代理对接受任何版本的公开声明将会永久性地授权您为函数库选择该版本。

org.slf4j

版权所有 (c) 2004-2008 QOS.ch 保留所有权利。

特此授权任何人免费获取本软件及相关文档文件（“软件”）的副本，用以无限制地处理软件，包括但不限于使用、复制、修改、合并、发布、分发、再许可和 / 或出售软件副本的权利，以及允许获得软件的个人按照下列条件执行这些操作：在软件的所有副本或主体部分应包含上述版权通知及本许可通告。软件“按原样”提供，不含任何形式的明确或隐含保证，包括但不限于适销性、特定用途适用性和非侵权的保证。在任何情况下，对于因软件、软件的使用或其他处理而引起或与之相关的任何索赔、损害或其他责任，无论是否基于合同或侵权行为，作者或版权持有人概不负责。

pcap

版权所有 © 1993, 1994, 1995, 1996, 1997, 1998, The Regents of the University of California

保留所有权利。

如果满足以下条件，便允许以源代码和二进制形式再分发和使用（包含或不含修改）：

- 源代码的再分发必须保留以上版权通告、本条件列表及以下免责声明。
- 二进制形式的再分发必须在分发所提供的文档和 / 或其他材料中复制以上版权通知、本条件列表及以下免责声明。
- 事先未获特定的书面同意，< 组织 > 或其责任者的名称不得用于认可或宣传本软件派生的产品。

本软件由版权持有人及责任者“按原样”提供，不含任何明确或隐含的保证，包括但不限于对适销性和特定用途适用性的隐含保证。对于因使用本软件而引起的任何形式的直接、间接、偶发、特殊、典型或随发损害（包括但不限于替代品或服务的采购；使用、数据或利润损失；或业务中断），无论基于任何原因或任何责任理论，例如合同、严格责任或民事侵权（包括疏忽等），< 版权持有人 > 概不负责，即使他们已被告知存在此类损害的可能性也一样。

zip4j

目录

1 概述

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

欢迎使用 Websense® Email Security Gateway，其为电子邮件系统提供最全面的保护，防止恶意威胁进入组织的网络。Email Security Gateway 托管在 Websense V-Series™（V 系列）设备（V10000 G2、V10000 G3 和 V5000 G2）上，可为组织提供全面的本地电子邮件安全。每封邮件都经过一套强大的防病毒和防垃圾邮件过滤器分析，以防受感染的电子邮件进入网络。基于域名和 IP 地址的邮件路由确保可靠、准确地传送电子邮件。

还可以使用 VMware 平台（ESXi v4.0 或更高版本）将 Email Security Gateway 作为虚拟设备进行部署。安装在单独的 Windows 计算机上的 TRITON 管理需要 Email Security Gateway 管理功能。虚拟设备安全模式仅限 Email Security。不支持双模式功能。有关部署和配置虚拟设备的完整信息，请参阅虚拟设备快速入门指南。

订阅 Websense Email Security Gateway Anywhere-可获得“云端”的混合服务预过滤功能，该功能可根据已知垃圾邮件数据库扫描传入的电子邮件。该功能通过阻止恶意电子邮件进入组织的网络，可节省网络带宽和维护成本。

可在您的 Email Security Gateway Anywhere 订购中增加 Websense ThreatScope（一组基于云的功能），增强您的安全性:

- URL 沙盒
- 文件沙盒
- 网络钓鱼检测

URL 沙盒对嵌入在 Email Security Gateway 入站邮件中、未分类的 URL 提供了实时分析。文件沙盒会检测通常含有安全威胁的电子邮件附件文件类型，包括（.exe、.pdf、.xls、.xlsx、.doc、.docx、.ppt、.pptx，以及存档文件）。有关这些功能的详细信息，请参阅 *URL 沙盒*（第 88 页）和 *Websense ThreatScope*（第 118 页）。网络钓鱼检测和教育针对网络钓鱼电子邮件的特征为入站邮件提供基于云的分析。用于处理可疑网络钓鱼邮件的选项包括阻止传送该邮件或使用网络钓鱼教育邮件替换该邮件。有关详细信息，请参阅网络钓鱼检测和教育（第 90 页）。

它与 Websense Data Security 相集成，为组织最敏感的数据提供可靠的保护，并有助于进行邮件加密。在 Data Security 中配置数据泄露防护策略，以启用在 Email Security Gateway **Settings（设置）> Inbound/Outbound（入站 / 出站）> Encryption（加密）**页面中配置的邮件加密选项。

如果您的网络中包含 Websense Web Security，也可以使用其 URL 分析功能。Email Security Gateway 会查询 Websense URL 类别主数据库并确定邮件中发现的 URL 的风险级别。有关信息，请参阅使用 *Web Security* 的 *URL* 扫描（第 43 页）。

日志记录和报表功能使企业能够查看系统状态，生成有关系统和电子邮件流量活动的报表。

Personal Email Manager 工具允许经授权的最终用户管理已被 Email Security 策略阻止但实际是可以安全地进行传送的电子邮件。最终用户可维护个人的“Always Block（始终阻止）”和“Always Permit（始终允许）”电子邮件地址列表，从而简化邮件传送。

主题:

管理员帮助文档概述

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Manager 帮助包括以下主题:

主题	标题	说明
1	概述	包括对 Websense Email Security Gateway、管理器帮助内容以及 Websense 技术支持联系信息的简要介绍
2	入门指南	概述首次配置向导、导航说明和提示、仪表盘定制、过滤数据库更新信息、混合服务的注册说明和 Data Security 数据泄露防护
3	配置系统设置	包括有关配置管理员角色、用户目录、域和 IP 地址组、设备集群和系统警报，以及 Email Security 管理器备份与恢复功能的详细信息
4	管理邮件	包含有关设置邮件属性、目录搜集攻击和转发控制选项、创建邮件路由和队列以及处理异常邮件和加密的信息
5	使用过滤器和策略	提供有关过滤器、过滤器操作、策略以及全局“Always Block（始终阻止）”和“Always Permit（始终允许）”列表的说明

主题	标题	说明
6	使用报表	包括有关报告首选项选项、演示报表生成和管理以及日志数据库设置的概述
7	配置 Personal Email Manager 最终用户选项	提供有关设置 Personal Email Manager 最终用户选项的信息，包括通知邮件的内容以及最终用户是否能够管理个人的阻止和允许列表；还包含有关最终用户门户外观的详细信息

嵌入式帮助

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 TRITON® 控制台模块托盘中，单击屏幕右上角的 **Help（帮助）**按钮可访问 Email Security Gateway 的嵌入式帮助。

单击 **Help（帮助）> Explain This Page（解释本页）**以打开与当前活动的 Email Security Gateway 屏幕相关的帮助。

重要事项

默认的 Microsoft Internet Explorer 设置可能会阻止帮助系统的运行。如果出现安全警告，请选择 **Allow Blocked Content（允许阻止的内容）**以显示帮助。

如果组织的安全标准允许，可以在 **Tools（工具）> Internet Options（Internet 选项）**界面的 Advanced（高级）选项卡中永久禁用警告消息。（在 Security（安全）选项下选中 **Allow active content to run in files on My Computer（允许活动内容在我的计算机上的文件中运行）**。）

单击 **Help（帮助）> Help Contents（帮助目录）**以显示完整的 Email Security Gateway 嵌入式帮助。若要在帮助查看程序中查找某个帮助主题，请选择下列选项卡之一：

- **Contents（目录）**

  双击书形图标可展开该手册的主题。

  单击目录条目可显示相应的主题。

- **Index（索引）**

  选择一个字母并滚动浏览列表。一个主题可能含有多个索引条目。

  双击条目可显示相应的主题。

- **Search（搜索）**

  输入关键字或短语，然后单击 **Go（执行）**。

  单击结果列表中的条目可显示相应的主题。

寻找答案门户

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Gateway 管理器的右侧窗格中包含一个 Find Answers（寻找答案）门户，可能包含以下组成部分:

- Top Picks（精选信息）部分，包含访问屏幕内容相关信息的外部链接
- Show Me How（操作指导）部分，为执行当前屏幕上或与当前屏幕相关的任务提供屏幕逐步说明
- Search（搜索）字段，可以用来在 Websense eSupport 中查找感兴趣的主题

Websense 技术支持

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 TRITON 控制台模块托盘中单击 **Help（帮助）> Support Portal（支持门户）**可访问 Websense 在线支持网站。Websense 软件和服务的相关技术信息随时可用，包括:

- 可搜索的 Websense 知识库（包括解决方案中心、技术文档库和客户论坛）
- 网络研讨会，以及指导视频
- 产品文档和深入的技术论文
- 常见问答

如有其他问题，请单击页面顶部的 **Contact Support（联系支持）**选项卡。

联系页面包含用于查找解决方案、打开在线支持案例和呼叫 Websense 技术支持的信息。

要更快地获得电话回应，请使用您的 **Support Account ID（支持帐户 ID）**，在 MyWebsense 的 Profile（个人资料）部分可以找到此 ID。

对于电话请求，请准备好:

- Websense 订购序列号
- 访问解决方案的管理控制台（例如 TRITON 控制台或设备管理器）
- 访问运行报告工具的机器和数据库服务器（Microsoft SQL Server 或 SQL Server Express）
- 熟悉您的网络体系结构，或有专家在场指导

2 入门指南

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

主题:

使用首次配置向导

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在安装后第一次使用 Email Security 时，可以使用配置向导。此向导帮助您在打开 Email Security 管理器用户界面之前快速轻松地完成关键配置。

单击 TRITON 控制台模块区的 Email Security 选项卡，将会显示一个弹出框，让您输入 Email Security 订购序列号。您可在此输入订购序列号，也可以跳过此步骤，以后通过 **Settings（设置）> General（一般）> Subscription（订购）**输入订购序列号（请参阅输入并查看订购信息（第 8 页））。

在订购序列号弹出框中单击 **OK（确定）**后，弹出的消息框可用于打开配置向导或 Email Security Gateway 仪表盘。

> **注**
>
> 如果选择打开 Email Security Gateway 仪表盘而非配置向导，接下来可选择打开一个文档，其中包含一些有用的配置设置信息。
>
> 如果决定跳过配置向导，以后将无法在此设备上访问该向导。

您可以在 Email Security 首次配置向导中输入以下信息:

- *全限定域名 (FQDN)*（第 6 页）
- *基于域的路由*（第 7 页）
- *入站邮件的受信任 IP 地址*（第 7 页）
- *Email Security Log Server 信息*（第 7 页）
- *Email Security 系统通知电子邮件地址*（第 8 页）

要保存您的设置，必须在向导的 Confirmation（确认）页面中进行检查，然后单击 **Complete（完成）**。

请注意，一旦在配置向导中单击了 **Cancel（取消）**，您在此之前输入的所有设置都会丢失。

向导结束时的 **Confirmation（确认）**页面可用于查看您的所有设置并根据需要对其进行修改。单击要修改项目旁边的 **Edit（编辑）**可查看相应的向导页面。在已编辑的页面中单击 **OK（确定）**返回 Confirmation（确认）页面。

在完成配置设置后单击 **Complete（完成）**。Email Security Gateway 仪表盘将会打开。

全限定域名 (FQDN)

配置向导的 FQDN 页面可用于指定设备的全限定域名 (FQDN)。该设置对于 Email Security Gateway 的正常工作非常重要。错误的全限定域名可能导致电子邮件流量中断。

在 **Fully Qualified Domain Name（全限定域名）**字段中输入设备的 FQDN（FQDN 格式为 appliancehostname.parentdomain.com）。

该 FQDN 作为默认条目出现在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面上。

基于域的路由

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

配置向导的 **Domain-based Route（基于域的路由）**页面可用于指定需要保护的域，以及指定此域的 SMTP 服务器。您可以在 **Settings（设置）> Inbound/ Outbound（入站 / 出站）> Mail Routing（邮件路由）**页面中添加更多受保护的域。有关受保护域的信息，请参阅受保护域组（第 59 页）。

根据向导中的如下步骤指定受保护的域:

1. 在 **Route name（路由名称）**输入字段中输入路由名称。
2. 在 **Protected Domain Name（受保护的域名）**字段中指定一个受保护的域。
3. 在相应字段输入受保护域的 SMTP 服务器 IP 地址或主机名及端口号。
4. 如果希望电子邮件路由使用传输层安全性 (TLS) 加密传输，请勾选 **Use Transport Layer Security（使用传输层安全性）**复选框。
5. 勾选 **Require Authentication（需要身份验证）**复选框，要求用户输入用户名和密码凭证。输入要使用的用户名和密码。

入站邮件的受信任 IP 地址

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 Trusted Inbound Mail（受信任的入站邮件）页面中，可以创建无需过滤某些入站电子邮件的受信任 IP 地址列表。受信任的 IP 地址可能包括内部邮件服务器或受信任的合作伙伴邮件服务器。

在 **Trusted IP address（受信任的 IP 地址）**字段中输入 IP 地址，然后单击向右箭头将其添加至 **Trusted IP address list（受信任的 IP 地址列表）**。

选择要删除的地址，然后单击 **Remove（删除）**将其从受信任的 IP 地址列表中删除。

有关在 Email Security 中如何处理受信任 IP 地址的详细信息，请参阅管理域和 IP 地址组（第 58 页）。

Email Security Log Server 信息

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Log Server 接收系统事件和电子邮件过滤活动的记录。Log Database 将使用这些记录生成报表。在 **Log Server** 页面中输入 Log Server 的 IP 地址和端口号。单击 **Check Status（检查状态）**接收 Log Server 的可用信息。

Email Security 系统通知电子邮件地址

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

可以在 **Notifications（通知）**向导页面中指定您希望将系统通知邮件发送到的电子邮件地址。这个地址通常为管理员电子邮件地址。在 **Notification email address（通知电子邮件地址）**字段中输入所需的地址。

输入并查看订购信息

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

购买 Websense® Email Security Gateway 模块后，您应会通过电子邮件接收到 Email Security Gateway 订购密钥。如果在首次打开 Email Security 时未输入订购序列号，可在 **Settings（设置）> General（一般）> Subscription（订购）**页面中输入。该订购序列号可以在 1 台设备中输入，并会应用于受 Email Security 管理器控制的所有设备。

输入有效的订购序列号后，有效期和已订购的用户数将会显示。Subscribed Features（订购功能）列表中将显示已购买的功能。

每次收到新的订购序列号时，请在 **Subscription key（订购序列号）**字段中输入。如果您的订购包含 Websense Email Security Gateway Anywhere，每次输入新的订购密钥来建立混合服务连接时必须注册混合服务。

导航 Email Security 管理器

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security 管理器用户界面可分为 6 个主要区域:

- 横幅
- 模块区
- Email Security Gateway 工具栏
- 左侧导航窗格
- 右侧快捷方式窗格
- 内容窗格

TRITON Unified Security Center 横幅显示:

- 您当前的登录帐户
- Log Off（注销）按钮可用于结束管理会话

Email Security 管理器中显示的内容根据登录用户的权限而有所不同。例如，报表管理员无法查看服务器配置设置或策略管理工具。

此部分介绍具有超级管理员权限的用户可使用的功能。

模块托盘可用于启动 TRITON Unified Security Center 的其他模块。Websense Web Security 或 Data Security 用户可单击 **Web Security** 或 **Data Security** 打开 Websense Web Security 或 Data Security 模块。

模块托盘中的 Appliances（设备）按钮用于打开 Manage Appliances（管理设备）窗口，在此窗口中可添加或删除系统中的设备。

TRITON 的 Settings（设置）按钮可让您:

- 管理您的管理员帐户。
- 添加其他 TRITON 管理员并分配适当权限。
- 为 TRITON 管理员指定并配置需要的目录服务。
- 配置管理员帐户通知邮件详细信息。
- 为登录到 TRITON 控制台的管理员启用和配置双因素身份验证。
- 审计管理员登录尝试和对 TRITON 设置所作的更改。

更多信息请参阅 TRITON Unified Security Center 帮助。

在模块区也可访问 Explain This Page（解释本页）上下文帮助、完整的帮助系统内容、有用的初始配置设置信息以及 Websense 支持门户网站。

模块托盘正下方的 Email Security 工具栏用于切换左导航窗格中的 Main（主页）和 Settings（设置）选项卡。使用 Main（主页）选项卡可查看 Email Security 状态、报表及策略管理特性和功能。使用 Settings（设置）选项卡可执行系统管理任务。工具栏也包含系统设备的下拉菜单。

右侧快捷方式窗格中包含一个 Find Answers（寻找答案）门户，该门户可能包括与活动屏幕相关的主题链接和特定任务的分步式教程。利用搜索功能，您可以在 Websense eSupport 网站上查找相关信息。右侧窗格中还包含指向常见管理任务的链接。单击列表中的项目可跳转到用于执行该任务的页面。

左右导航窗格都可通过单击窗格顶部的双箭头（<< 或 > >）图标来最小化。单击相反图标（> > 或 <<）便可查看窗格。单击最小化后的左侧导航窗格上的快捷方式图标可以直接访问 Email Security 的各组功能，而无需最大化窗格。

Email Security Gateway 仪表盘

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

登录到 TRITON 控制台并连接到 Email Security 管理器时，首先出现的是 **Status（状态）> Dashboard（仪表盘）**页面的 **Value（值）**选项卡。该选项卡显示有关您网络中 Email Security Gateway 的值的信息，以及系统健康警报摘要。

显示的信息类型和详细程度取决于您的订购级别。例如，如果要求 Email Security Gateway Anywhere 显示有关电子邮件混合服务以及如何保护您系统的信息，则您必须购买 Websense ThreatScope 插件，才能查看有关 URL 或文件沙盒功能的指标。

仪表盘元素仅对超级管理员和有权在 Email Security 仪表盘上查看报表的委托管理员可见（请参阅管理管理员帐户（第 45 页））。

如果管理员对仪表盘作出更改（例如添加、删除和编辑图表，或将图表移至仪表盘的其他位置），则仪表盘右上区域的 **Save（保存）**按钮会激活。重命名选项卡也会激活 **Save（保存）**按钮。请确保从仪表盘导航至其他位置之前已保存任何更改。

除了值仪表盘选项卡，仪表盘还包括 2 个其他默认选项卡:

- 入站仪表盘显示入站电子邮件常见域和邮件收件人的图表。常见域和收件人信息根据邮件大小或数量排序。
- 出站仪表盘显示出站电子邮件常见发件人的图表，根据邮件大小或数量排序。此选项卡的其他默认图表显示整体出站邮件摘要以及包含嵌入式 URL 的出站邮件的摘要。

单击显示“加号”标志图标 (+) 的选项卡，可以添加新的自定义选项卡。在 Add Tab（添加选项卡）对话框中输入名称（最多 10 个字母数字字符，包括下划线）。单击 **Add Charts（添加图表）**将元素添加到新的选项卡。您最多可以添加 4 个自定义选项卡。

单击某个活动选项卡的编辑图标，可打开 Edit Tab（编辑选项卡）对话框，在此您可以更改选项卡名称。也可以单击 **Delete Tab（删除选项卡）**以删除选项卡。如果需要，可以重命名默认选项卡，但这些选项卡不能删除。

默认的 Value（值）、Inbound（入站）和 Outbound（出站）仪表盘各自每次最多可显示 12 个图表。可以自定义大多数仪表盘图表来更改时间段（例如，今天、最近 7 天、最近 30 天）和显示格式（例如，堆积柱形图、堆积面积图、多系列折线图）。可以在一个选项卡上包含同一图表的多个版本（例如，显示不同的时间段）。有关仪表盘显示的图表的列表，请参阅可用仪表盘图表（第 14 页）。

- 大多数仪表盘元素每 2 分钟更新一次。Health Alert Summary（健康警报摘要）每 30 秒更新一次。

  如果修改某个选项卡上的任何元素，则该选项卡上的所有其他元素也将更新。例如，如果更改一个图表的时间段，则会刷新页面上所有图表的数据。
- 可用的仪表盘元素集取决于您的订购类型。例如，与混合服务相关的图表仅可用于 Email Security Gateway Anywhere 部署。
- 要将元素添加到选项卡，单击 **Add Charts（添加图表）**，然后查看将元素添加到仪表盘选项卡（第 13 页）了解说明。
- 使用拖放功能将元素从一个选项卡上的一个位置移至同一选项卡上的不同位置。单击图表标题区，将图表拖至新的位置。
- 要从选项卡中删除一个元素，请单击元素标题栏中的 Options（选项）图标，然后选择 **Remove（删除）**。

- 要访问一个元素的所有编辑选项，请单击元素标题栏中的 Options（选项）图标，然后选择 **Edit（编辑）**。追溯功能也可用。您可以执行下列编辑操作:
  - 更改:
    - 图表名称
    - 图表类型
    - 时间段
    - 常见数字标号
  - 恢复默认图表设置
  - 复制图表（将图表添加到标题末尾带“(1)”的活动选项卡；选择 **Edit（编辑）**更改图表名称）
- 要打印图表，请单击 Options（选项）图标并选择 **Print（打印）**。您还可以右键单击图表，然后选择打印选项。
- 要查看图表的放大版本，请单击元素标题栏中的 Enlarge（放大）图标。您可以在此视图中访问一些编辑选项（例如，图表类型、时间段、常见数字标号）以及追溯功能。单击 **Print Chart（打印图表）**打印当前图表。单击 **Close（关闭）**时，在此视图中对图表所做的任何更改不会保留在仪表盘中。
- 单击饼图、条形图或折线图通常允许显示具有更多详细信息的追溯数据。例如，单击代表 24 小时期间的数据的图表元素可以 1 小时为增量显示相同的数据。这些功能在 Edit（编辑）、Enlarge（放大）和 Preview（预览）图表视图中可用。

仪表盘工具栏中出现两个按钮:

- **Add Charts（添加图表）**允许管理员通过将元素添加到页面，自定义所选仪表盘选项卡视图。请参阅将元素添加到仪表盘选项卡（第 13 页）。
- **Print（打印）**用于打开一个辅助窗口，其中显示页面中图表的可打印版本。请使用浏览器选项打印此页。

值仪表盘

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Value（值）仪表盘显示警报消息以及反映电子邮件保护系统当前状态的图表，内容集中于网络中的电子邮件流量活动。默认选项卡元素包括以下内容:

- **Health Alert Summary（健康警报摘要）**显示 Websense 软件的状态。单击错误或警告消息可打开 Alerts（警报）页面，其中包含更详细的警报信息（请参阅查看系统警报（第 16 页））。
- 在 **24-Hour Business Value（24 小时业务数据）**图表中，可以查看 Email Security Gateway 在过去 24 小时通过阻止可疑电子邮件流量来保护网络的统计数据。数据包括按分析结果列出的已阻止连接和邮件总数、电子邮件分析的误报与遗漏垃圾邮件结果数，以及 Email Security Gateway 处理的各类邮件总数。

- **30-Day Blocked Message Estimated Savings（30 天被阻止邮件预计节省）**图表提供 Email Security Gateway 分析得出的成本节省估算值，这可阻止不需要的邮件和威胁（包括在连接层）、保护网络资源，并节省组织的时间和金钱。增加电子邮件混合服务（一种 Email Security Gateway Anywhere 环境）后，受到感染的流量在进入网络之前将被拦截，可节约更多成本。

  将鼠标悬停在预计节省项目上，即可查看混合服务和 Email Security Gateway 电子邮件分析所节省的大致成本。每 MB 流量成本的默认值包括预防威胁和垃圾邮件预计节省的成本以及最终节约的带宽。单击元素标题栏中的 Options（选项）图标，然后选择 **Edit（编辑）**设置每 MB 被阻止邮件所节省的成本。

- 在 **30-Day Blocked Message Value（30 天被阻止邮件数据）**中，可查看类似于 24 小时值图表的指标，并展示前 30 天的 Email Security Gateway 保护。此图表显示被阻止连接和邮件的总数及所占百分比，包括电子邮件分析的误报与遗漏垃圾邮件结果数各占的百分比。

您可以重命名默认选项卡，但不能删除。您可以删除选项卡上显示的任何图表，然后单击 **Add Charts（添加图表）**将不同的图表添加到选项卡。

入站仪表盘

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Inbound（入站）仪表盘提供有关流入 Email Security Gateway 的入站邮件流量的摘要数据。默认图表包括以下内容:

- **Top Inbound Domains by Message Size（按邮件大小划分的常见入站域）**图表显示大多数入站邮件来源的邮件域，并按邮件大小绘制。
- **Top Inbound Domains by Message Volume（按邮件数量划分的常见入站域）**图表显示占所有入站邮件多数的邮件域。
- **Top Inbound Recipients by Message Size（按邮件大小划分的常见入站收件人）**图表显示收到大多数入站电子邮件的收件人地址，并按邮件大小绘制。
- **Top Inbound Recipients by Message Volume（按邮件数量划分的常见入站收件人）**图表显示流入 Email Security Gateway 的所有入站电子邮件中的大多数邮件的收件人地址。

您可以重命名默认选项卡，但不能删除。您可以删除选项卡上显示的任何图表，然后单击 **Add Charts（添加图表）**将不同的图表添加到选项卡。

出站仪表盘

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Outbound（出站）仪表盘提供有关流入 Email Security Gateway 的出站邮件流量的摘要数据。默认图表包括以下内容:

- **Top Outbound Senders by Message Size（按邮件大小划分的常见出站发件人）**图表显示占多数出站电子邮件的发件人地址，并按邮件大小绘制。
- **Top Outbound Senders by Message Volume（按邮件数量划分的常见出站发件人）**图表显示代表所有出站邮件中大多数邮件的发件人地址。
- **Outbound Messages Summary（出站邮件摘要）**图表显示 Email Security Gateway 处理的出站邮件的总数，并按邮件分析结果排序（清洁、病毒、垃圾邮件等）。
- **Outbound Message Embedded URL Summary（出站邮件嵌入式 URL 摘要）**图表显示包含至少 1 个嵌入式 URL 的分析出站邮件的百分比，按邮件分析结果显示。例如，如果 50 个出站邮件被确定为垃圾邮件，并且其中 40 个包含嵌入式 URL，则此图表中所示的垃圾邮件类型的百分比为 80% (40/50)。

您可以重命名默认选项卡，但不能删除。您可以删除选项卡上显示的任何图表，然后单击 **Add Charts（添加图表）**将不同的图表添加到选项卡。

将元素添加到仪表盘选项卡

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用 **Status（状态）> Dashboard（仪表盘）> Add Charts（添加图表）**页面将元素添加到 Value（值）、Inbound（入站）、Outbound（出站），或任何自定义仪表盘选项卡。

要开始，请使用 **Add elements to tab（将元素添加到选项卡）**下拉列表，选择一个选项卡，然后选择您要从 **Dashboard Elements（仪表盘元素）**列表添加的元素。**Restore Tab Defaults（恢复选项卡默认值）**按钮位于 Available Tabs（可用选项卡）部分，仅适用于默认选项卡，不适用于自定义选项卡。

- 您可以将元素添加到任何选项卡。
- 每个选项卡都可以显示最多 12 个元素。
- 所选选项卡当前显示的元素标有蓝色圆圈图标。
- 可以将同一元素的多个副本添加到一个选项卡（例如，每一个可能会显示一个不同的时间段）。

在列表中选择一个元素时，**Preview（预览）**窗格中会显示样品。您可以使用预览窗格更改图表 **Name（名称）**，以及（如适用）**Chart type（图表类型）**、**Time period（时间段）**和 **Top（最高）**值（例如，最多 1-5 个类别，或最多 16-20 个用户）。图表名称可长达 47 个字母数字字符（包括空格和下划线）。

- **Chart type（图表类型）：**很多图表可以显示为多系列条形图、柱形图或折线图，也可显示为堆积面积图或柱形图。有些可以显示为条形图、柱形图、折线图或饼图。可用的类型取决于所显示的数据。
- **Time period（时间段）：**大多数图表可以显示可变的时间段：今天（当天午夜以后的期间）、最近 7 天，或最近 30 天。
- **Top（最高）：**显示有关常见用户、类别、URL 等的信息的图表，最多可显示 5 个值。选择是否显示最多 5 个值、6-10 个值、11-15 个值或 16-20 个的值。

完成更改后，单击 **Add（添加）**。仪表盘选项卡会立即更新。

如果您在编辑图表并想重新开始，请单击 **Restore Defaults（恢复默认值）**将图表重置为默认的时间段、类型和最高值（如果有）。

可用仪表盘图表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

以下表中的仪表盘图表位于 Add Charts（添加图表）页面 Dashboard Elements（仪表盘元素）列表中。

有些图表可能会显示用户名或 IP 地址等潜在敏感信息。因此请确保您选择的图表适合所有具备查看权限的管理员查看。

图表名称
30-Day Blocked Message Value（30 天被阻止邮件数据）
30-Day Blocked Message Estimated Savings（30 天被阻止邮件预计节省）
24-Hour Business Value（24 小时业务数据）
Connections Summary（连接摘要）
Inbound Messages Summary（入站邮件摘要）
Outbound Messages Summary（出站邮件摘要）
Average Message Volume in Work Queue（工作队列中的平均邮件数量）
Data Security Policy Violations by Severity（按严重性划分的数据安全策略违规）
Top Data Security Policy Violations（常见数据安全策略违规）
Top Outbound Senders by Message Size（按邮件大小划分的常见出站发件人）
Top Outbound Senders by Message Volume（按邮件数量划分的常见出站发件人）
Top Blocked Protected Domain Addresses（被阻止的常见受保护域地址）
Top Inbound Domains by Message Size（按邮件大小划分的常见入站域）

图表名称
Top Inbound Domains by Message Volume（按邮件数量划分的常见入站域）
Top Inbound Recipients by Message Size（按邮件大小划分的常见入站收件人）
Top Inbound Recipients by Message Volume（按邮件数量划分的常见入站收件人）
Inbound Message Embedded URL Summary（入站邮件嵌入式 URL 摘要）
Outbound Message Embedded URL Summary（出站邮件嵌入式 URL 摘要）
Inbound Message Embedded URL Categories（入站邮件嵌入式 URL 类别）
Outbound Message Embedded URL Categories（出站邮件嵌入式 URL 类别）
Top Inbound Targeted Phishing Attacks（常见入站针对性网络钓鱼攻击）
Top Inbound Phishing Attack Victims（常见入站网络钓鱼攻击受害者）
Inbound Message Throughput（入站邮件吞吐量）
Outbound Message Throughput（出站邮件吞吐量）
Outbound Encrypted Messages Summary（出站加密邮件摘要）
（按方向划分的邮件数量）
常见入站发件人
入站垃圾邮件数量
入站垃圾邮件百分比
入站病毒数量
入站病毒百分比
入站商业群发电子邮件数量
入站商业群发电子邮件百分比
出站垃圾邮件数量
出站垃圾邮件百分比
出站病毒数量
出站病毒百分比
按邮件类型划分的入站数量
按邮件类型划分的出站数量
随机 TLS 使用数量
通过强制 TLS 渠道的常见收件人域
常见强制 TLS 使用失败数量
入站 ThreatScope 分析数量（需要 Websense ThreatScope 插件）
ThreatScope 检测到的所收到的常见附件数量（需要 Websense ThreatScope 插件）
ThreatScope 检测到的按文件类型划分的附件数量（需要 Websense ThreatScope 插件）
受 ThreatScope 保护的常见收件人（需要 Websense ThreatScope 插件）
混合服务邮件大小摘要（适用于 Email Security Gateway Anywhere 部署）
混合服务邮件数量摘要（适用于 Email Security Gateway Anywhere 部署）

查看系统警报

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

仪表盘中的 **Health Alert Summary（健康警报摘要）**显示 Email Security 软件的状态。单击错误或警告消息可打开 **Status（状态）> Alerts（警报）**页面，其中提供更详细的警报信息。

Alerts（警报）页面显示影响 Email Security 软件健康状况的问题相关信息，提供指向故障排除帮助的链接，并记录最近实时过滤数据库更新的详细信息。

Active Alerts（活动警报）列表显示受监控 Websense 软件组件的状态。有关哪些组件被监控的详细信息，请单击警报消息列表上方的 **What is monitored?（被监控组件？）**。

要排除问题，请单击错误或警告消息旁边的 **Solutions（解决方案）**。单击 **Learn More（更多信息）**了解有关该类警报的详细内容。

Websense 健康警报

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Health Alert Summary（健康警报摘要）将列出 Websense 软件被监控组件遇到的任何潜在威胁。下列情况下将会生成警报:

- 使用期限问题或订购序列号问题
- Email Security 服务不可用或无法运行
- Email Security 配置问题
- 主数据库服务器连接问题
- 过滤数据库引擎和下载问题
- URL 扫描服务器问题
- Log Server 不可用、无法运行或出现性能问题
- Email Security、Log Server 或 Log Database 版本不匹配
- Log Database 不可用或有性能问题
- 磁盘空间不足问题
- 过时的系统日志或邮件队列文件
- 系统日志或邮件队列不可用
- 第三方加密应用问题
- 设备群集连接和同步问题
- 用户目录服务器不可用或无法运行
- 用户目录凭证无效

如果您已订购 Websense Email Security Gateway Anywhere，或者您的订购中包含电子邮件和数据安全组件，Websense 软件将监控协同操作的组件以在下列情况下提供警报：

- Websense Data Security 管理器注册、配置和连接状态
- 混合服务注册、身份验证和连接状态

警报消息旁边的图标指示相关情况下的潜在威胁。

消息只是提供信息，不能反映与安装有关的问题（例如成功的数据库下载或群集同步）。

警报的情况可能会造成问题，但不会立即阻止过滤或报表功能（例如，混合服务数据不可用或订购序列号即将过期）。

Websense 软件组件无法工作（未配置或无法运行，这可能会影响过滤或报表功能），或者订购序列号已经过期。

单击 Health Alert Summary（健康警报摘要）中的警报消息可进入 Alerts（警报）页面，其中提供有关当前警报情况的更多信息。单击 Learn More（更多信息）（对于信息类警报）或 Solutions（解决方案）（对于错误或警告）可查看详细信息和故障排除提示。

查看和搜索日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Gateway 包含若干日志，可帮助您监控系统及电子邮件状态。这些日志可按预定义的时间段搜索，您也可以自定义要搜索的时间段。邮件日志还可让您使用电子邮件地址、扫描结果或消息状态等搜索条件优化消息搜索。

您可以将任何日志的搜索结果导出到逗号分隔值 (CSV)、或 HTML 文件。请注意，导出的日志条目数量最多不能超过 100,000 条。

Email Security 包含以下日志：

- 邮件日志（第 18 页）
- 连接日志（第 22 页）
- 审计日志（第 24 页）
- *Personal Email Manager* 审计日志（第 26 页）
- 系统日志（第 28 页）
- 控制台日志（第 29 页）
- 混合服务日志（第 31 页）

邮件日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

邮件日志记录经 Email Security 处理的每封电子邮件（入站、出站和内部）的相关信息。从 **Main（主页）> Status（状态）> Logs（日志）**页面可访问邮件日志。

在日志表格横幅中的 **Per page（每页）**下拉列表中可以配置每个日志页面的日志条目数 (25-200)。在页面顶部和底部，按上一页或下一页箭头可滚动显示邮件日志的页面，也可以在 **Page（页面）**字段中输入具体的页码并单击 **Go（进入）**。

邮件记录在数据库中保存的时间长度取决于邮件数量和数据库分区容量。要保存邮件记录，请定期使用 Export（导出）选项导出日志。导出操作不会从邮件日志删除记录。它会将日志数据转换成 CSV 或 HTML 文件。

Message Log（邮件日志）页面出现时，会显示最近的记录。使用 **View from/to（查看从 / 至）**字段可指定要查看的日志条目的日期 / 时间范围。日历包括以下选项:

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。

邮件日志数据

将收集以下邮件数据并以表格形式显示:

邮件数据项目	说明
Message Log ID（邮件日志 ID）	数据库生成的邮件标识符
Received Date/Time（接收日期 / 时间）	接收邮件的日期和时间
Subject（主题）	邮件主题
Sender Address（发件人地址）	发件人电子邮件地址
Sender IP（发件人 IP）	邮件发件人 IP 地址
Recipient Address（收件人地址）	收件人电子邮件地址。如果邮件有多个收件人，则显示第一个收件人地址。

邮件数据项目	说明
Scanning Result（扫描结果）	邮件过滤结果（安全、病毒、垃圾邮件、数据使用、异常、商业群发电子邮件、网络钓鱼或自定义内容）。Data Security 策略显示时，此列中的 **View Incident（查看事件）**链接可以打开 Data Security 中的事件详细信息。
Message Status（邮件状态）	当前邮件状态（已发送、发送延迟、停止发送、异常、发送失败、等待发送，或等待邮件分析）。根据采用的策略，有多个收件人的邮件可能会有多个状态条目。

邮件收件人详细信息

单击单个邮件日志标识符时，将会显示邮件详细信息。以下邮件详细项目将会以表格形式显示:

详细项目	说明
Recipient Address（收件人地址）	收件人电子邮件地址。如果邮件有多个收件人，此栏将有多个条目。
Recipient IP（收件人 IP）	邮件收件人 IP 地址
Direction（方向）	邮件方向（入站、出站或内部）。如果邮件有多个收件人，此栏可能有多个条目。
Delivered Date/Time（发送日期 / 时间）	邮件发送的日期和时间
Policy（策略）	邮件所用策略的名称。如果邮件有多个收件人，此栏可能有多个条目。
Rule（规则）	邮件所用策略规则的名称。如果邮件有多个收件人，此栏可能为一封邮件显示多个条目。 如果邮件的扫描结果为安全，该项目可能为空白。
Scanning Result（扫描结果）	邮件过滤结果（安全、病毒、垃圾邮件、数据使用、异常、商业群发电子邮件、网络钓鱼或自定义内容）
Message Status（邮件状态）	当前邮件状态（已发送、发送延迟、停止发送、异常或发送失败）
Quarantined?（已隔离？）	指示邮件是否已隔离（Yes（是）或 No（否））。已被 Data Security 隔离的邮件将显示 **View Incident（查看事件）**链接。

邮件日志详细信息

单击 Message Log ID（邮件日志 ID）列中的邮件以查看收件人详细信息时，页面底部将出现新按钮 **View Log Details（查看日志详细信息）**。邮件日志详细信息将出现在表格中，包括收到的日期和时间列以及邮件详细信息来源列。详细信息来源可能包含邮件和连接控制数据、电子邮件策略数据及传送数据。

日志详细信息显示在第三列，可能包含下列相关信息:

- 邮件大小、发件人和收件人
- 连接类型、发件人 IP 地址以及接收连接请求的 Email Security 设备
- 应用的电子邮件策略和操作，包括策略和规则名称（过滤器和操作）、电子邮件方向（入站、出站或内部）、遇到的病毒或垃圾邮件名称以及根据过滤结果采取的操作
- 混合服务扫描结果，包括 DKIM 验证（如果适用）
- 邮件传送处理，包括收件人电子邮件和 IP 地址、加密类型及传送状态

邮件日志搜索选项

邮件日志包含多个搜索选项，包括日期范围或关键字搜索。在 **View from/to（查看自 / 至）**字段日历控件中选择日期，以确定搜索的日期 / 时间范围。**from（自）**或 **to（至）**字段的默认值是您打开日志的日期和时间。

进行关键字搜索时，可从 **Keyword search（关键字搜索）**下拉列表中选择要搜索的日志元素，然后在列表右边的字段中输入搜索词。在所有邮件日志元素中搜索关键字，或在下列任一邮件日志组件中搜索:

- Message Log ID（邮件日志 ID）
- Subject（主题）
- Sender Address（发件人地址）
- Sender IP（发件人 IP）
- Recipient Address（收件人地址）
- Scanning Result（扫描结果）
- Message Status（邮件状态）

支持在关键字中使用通配符条目 (*)。但是，对于发件人 IP 地址，必须将星号通配符条目放置在地址条目末尾，即句点后（例如 10.0.*）。

单击 **Set to Default（设置为默认）**将关键字搜索选项恢复为默认设置（所有邮件日志组件和关键字字段为空白）。

单击 Keyword（关键字）搜索框右边的 **Advanced Options（高级选项）**查看可用于缩小邮件搜索范围的高级搜索选项。从下列一个或多个类别中选择选项以优化搜索:

类别	说明
By Email Address （按电子邮件地址）	单击 **Specify Email Addresses（指定电子邮件地址）**打开 Specify Email Addresses（指定电子邮件地址）对话框。指定匹配条件，包括电子邮件地址；地址是发件人地址、收件人地址还是两者。搜索结果包括在 Condition Details（条件详细信息）框中输入的任何地址的匹配项。不支持通配符条目。 请用分号 (;) 分隔电子邮件地址条目。
By Scanning Result （按扫描结果）	按邮件过滤结果搜索（安全、病毒、垃圾邮件、商业群发电子邮件、数据使用、自定义内容、异常、阻止列表、网络钓鱼或 ThreatScope） “阻止列表”类型适用于被 Personal Email Manager 始终阻止列表阻止的邮件。
By Message Status （按邮件状态）	按当前邮件状态搜索（已发送、发送延迟、停止发送、异常、已过期或发送失败）

单击 **Search（搜索）**生成搜索结果。

单击 **Set to Default（设置为默认）**将所有搜索选项设置恢复为默认状态。

邮件日志导出选项

要导出邮件日志搜索结果:

1. 单击 **Export（导出）**打开 Export Log（导出日志）对话框。
2. 选择所需的输出文件类型（CSV 或 HTML）。
   - 如果选择 **CSV**，将打开一个对话框，让您以 CSV 格式打开或保存文本文件。
   - 如果选择 **HTML**，将打开一个对话框，让您打开或保存包含日志数据的 HTML 文件。
3. 选择要导出的页面（所有页面、当前页面或页面范围）。
4. 单击 **OK（确定）**。

连接日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

连接日志记录 Email Security 的传入连接请求和连接扫描结果。在 **Main（主页）> Status（状态）> Logs（日志）**页面上单击 **Connection（连接）**选项卡访问连接日志。

在日志表格横幅中的 **Per page（每页）**下拉列表中可以配置每个日志页面的日志条目数 (25-200)。在页面顶部和底部，按横幅中的上一页或下一页箭头可滚动显示连接日志的页面，也可以在 **Page（页面）**字段中输入具体的页码并单击 **Go（进入）**。

连接记录在数据库中保存的时间长度取决于连接量和数据库分区容量。要保留连接记录，请定期使用 Export（导出）选项导出日志数据。导出操作不会从连接日志删除记录。它会将日志数据复制到 CSV 或 HTML 文件。

Connection Log（连接日志）页面出现时，会显示最近的记录。使用 **View from/to（查看从 / 至）**字段可指定要查看的日志条目的日期 / 时间范围。日历包括以下选项:

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。

连接日志数据

将收集以下连接数据并以表格形式显示:

连接数据项目	说明
Sender IP Address（发件人 IP 地址）	连接的发件人 IP 地址
Date/Time（日期 / 时间）	接收连接的日期和时间
Number of Messages（邮件数量）	连接中的邮件数量
Security Level（安全等级）	加密或未加密

连接数据项目	说明
Connection Status （连接状态）	当前连接状态（已接受或已阻止）。 状态详细信息显示在悬停弹出框中。 可能的 **Blocked（已阻止）**状态详细信息如下所示: • 在 SMTP 服务器问候语之前收到 HELO/EHLO • 来自 < 服务器地址 > 的连接未通过 SPF 检查。 • 反向 DNS 查找失败。 • 来自 < 服务器地址 > 的同时连接数超出限制。 • 邮件数量超出限制。 • 邮件大小超出限制。邮件已转发至 < 队列 *ID*> 队列。 • 文件大小超出限制。邮件已转发至 < 队列 *ID*> 队列。 • 每次连接的数据大小超出限制。邮件已转发至 <队列 *ID*> 队列。 • HELO 命令语法错误 • EHLO 命令语法错误 • 无效收件人的百分比超出限制。 • <服务器名称 > 的连接尝试未能通过全局 Always Block（始终阻止）列表检查。 • <服务器名称 > 的连接尝试未能通过收件人验证检查。 • <服务器名称 > 的连接尝试未能通过用户身份验证。 • 来自 < 发件人名称 > 的开放转发被阻止。 可能的 **Accepted（已接受）**状态详细信息如下所示: • 混合服务 IP 组条目匹配 • 受信任的 IP 组条目匹配 • 访问列表条目匹配 • 全局始终允许列表条目匹配 • BATV 绕过条目匹配 • 真实源 IP 地址与受信任的 IP 组条目匹配 • 真实源 IP 地址与访问列表条目匹配 • 真实源 IP 地址与混合服务 IP 组条目匹配 • 真实源 IP 地址与全局始终允许列表条目匹配 • 真实源 IP 地址与 BATV 绕过条目匹配

单击连接日志中的单个发件人 IP 地址链接时，邮件日志将会打开，并显示与所选连接相关的一个或多个邮件的详细信息。有关详细信息，请参阅邮件日志数据（第 18 页）。

连接日志搜索选项

连接日志包含多个搜索选项，包括日期范围或关键字搜索。在 **View from/to（查看自 / 至）**字段日历控件中选择日期，以确定搜索的日期 / 时间范围。**from（自）**或 **to（至）**字段的默认值是您打开日志的日期和时间。

进行关键字搜索时，可从 **Keyword search（关键字搜索）**下拉列表中选择要搜索的日志元素，然后在列表右边的字段中输入搜索词。在所有连接日志元素中搜索关键字，或在下列任一组件中搜索:

- Sender IP address（发件人 IP 地址）（关键字不支持通配符和特殊字符）
- Security Level（安全等级）
- Connection Status（连接状态）

单击 **Search（搜索）**生成搜索结果。

单击 **Set to Default（设置为默认）**将关键字搜索选项恢复为默认设置（**所有**包含关键字字段的连接日志组件为空白）。

连接日志导出选项

要导出连接日志搜索结果:

1. 单击 **Export（导出）**打开 Export Log（导出日志）对话框。
2. 选择所需的输出文件类型（CSV 或 HTML）。
   - 如果选择 **CSV**，将打开一个对话框，让您以 CSV 格式打开或保存文本文件。
   - 如果选择 **HTML**，将打开一个对话框，让您打开或保存包含日志数据的 HTML 文件。
3. 选择要导出的页面（所有页面、当前页面或页面范围）。
4. 单击 **OK（确定）**。

审计日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Websense Email Security Gateway 提供审计跟踪，显示使用过 Email Security 管理器的管理员以及对策略和设置的任何更改。此类信息仅限超级管理员访问。通过审计日志监控管理员的更改，可确保根据组织认可的使用策略负责任地处理系统控制。

单击 **Main（主页）> Status（状态）> Logs（日志）**页面的 Audit Log（审计日志）选项卡可查看审计日志，以及根据需要将所选部分导出为 CSV 或 HTML 文件。

审计记录保存期为 30 天。要使审计记录保持时间超过 30 天，请定期使用 Export（导出）选项导出日志。导出操作不会从审计日志删除记录。它会将日志数据转换成 CSV 或 HTML 文件。

Audit Log（审计日志）页面打开时，会显示最近的记录。使用日志上方的 **View（查看）**下拉列表选项选择要查看的日志条目范围：All（所有）、One Day（一天）、One Week（一周）、One Month（一个月）或 Custom（自定义）。选择 **Custom（自定义）**时，使用 **View from/to（查看自 / 至）**字段可指定要查看的日志条目的所需日期 / 时间范围。日历包括以下选项：

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。

在 View（查看）选项下面，从 **Per page（每页）**下拉列表中选择希望每个日志页面显示的日志条目数（25 至 200）。默认值为 25。在页面顶部和底部，使用上一页或下一页箭头可滚动显示日志，也可以在 **Page（页面）**字段中输入要查看的页面并单击 **Go（进入）**。

审计日志数据

日志以表格形式显示下列系统审计信息：

列	说明
Date（日期）	更改的日期和时间（根据时区而调整）。 为确保审计日志中数据的一致性，请确保运行 Websense 组件的机器的日期和时间设置是同步的。
User（用户）	做出更改的管理员用户名
Server（服务器）	受更改影响的设备 IP 地址
Client（客户端）	进行更改的管理员机器的 IP 地址
Role（角色）	管理员角色（超级管理员、审计员、隔离管理员、报表管理员、安全管理员、策略管理员或组报表管理员）
Type（类型）	Email Security 用户界面中的更改位置（例如，如果输入新的订购序列号，此列会显示 **General Settings（一般设置）| Subscription（订购）**）
Element（元素）	发生更改的特定动态对象（如果有）的标识符
Action（操作）	更改的类型（例如添加、删除、更新、导入、导出、移动、身份验证、同步或重置）
Action Detail（操作详细信息）	用于打开 Details（详细信息）消息框的链接，消息框中显示所做更改的相关信息

审计日志导出选项

要导出审计日志记录:

1. 从 **Export range（导出范围）**下拉列表选择时间段（当前页面、最近 24 小时、最近 7 天或最近 30 天）。

   选择 **Last 30 days（最近 30 天）**导出整个审计日志文件。
2. 单击 **Go（执行）**。
3. 在 **Export Log（导出日志）**对话框中选择所需的输出文件类型。
   - 如果选择 **CSV**，将打开一个对话框，让您以 CSV 格式打开或保存文本文件。
   - 如果选择 **HTML**，将打开一个对话框，让您打开或保存包含日志数据的 HTML 文件。
4. 单击 **OK（确定）**。

Personal Email Manager 审计日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Personal Email Manager 审计日志记录由 Personal Email Manager 通知邮件或隔离邮件列表执行的最终用户的电子邮件管理活动。单击 Personal Email Manager 选项卡，在 **Main（主页）> Status（状态）> Logs（日志）**页面访问 Personal Email Manager Audit Log（Personal Email Manager 审计日志）。

在日志表格横幅中的 **Per page（每页）**下拉列表中可以配置每个日志页面的日志条目数 (25-200)。在页面顶部和底部，按上一页或下一页箭头可滚动显示 Personal Email Manager 审计日志的页面，也可以在 **Page（页面）**字段中输入具体的页码并单击 **Go（进入）**。

邮件记录在数据库中保存的时间长度取决于邮件数量和数据库分区容量。要保存邮件记录，请定期使用 Export（导出）选项导出日志。导出操作不会从 Personal Email Manager 审计日志删除记录。它会将日志数据转换成 CSV 或 HTML 文件。

当出现 Personal Email Manager Audit Log（Personal Email Manager 审计日志）页面时，会显示最近的记录。使用日志上方的 **View（查看）**下拉列表选项选择要查看的日志条目范围：All（所有）、One Day（一天）、One Week（一周）、One Month（一个月）或 Custom（自定义）。选择 **Custom（自定义）**时，使用 **View from/to（查看自 / 至）**字段可指定要查看的日志条目的日期 / 时间范围。日历包括以下选项:

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。

Personal Email Manager 审计日志数据

将收集以下数据并以表格形式显示:

邮件数据项目	说明
Date（日期）	在 Personal Email Manager 中，在邮件上执行操作的日期和时间
User Name（用户名）	执行邮件操作的 Personal Email Manager 用户的电子邮件地址
End-user Action（最终用户操作）	在 Personal Email Manager 中，在邮件上执行的操作（Deliver（传送）、Delete（删除）和 Reprocess（重新处理），不包括 Add to Always Block List（添加到始终阻止列表）、Add to Always Permit List（添加到始终允许列表），或 Download（下载）等操作）
Message ID（邮件 ID）	数据库生成的邮件标识符。有多个收件人的邮件的“邮件 ID”可能会在日志中多次出现。
End-user Action Status（最终用户操作状态）	指示 Personal Email Manager 最终用户操作是否成功完成（成功或失败）

Personal Email Manager 审计日志搜索选项

进行关键字搜索时，可从 **Keyword search（关键字搜索）**下拉列表中选择要搜索的日志元素，然后在列表右边的字段中输入搜索词。在下列其中一种 Personal Email Manager 审计日志元素中搜索关键字:

- Message ID（邮件 ID）
- User Name（用户名）

在 **Appliance（设备）**下拉列表中指定您要在其上执行搜索的设备。默认条目为活动设备。

单击 **Set to Default（设置为默认）**将关键字搜索选项恢复为默认设置（关键字字段为空白）。

Personal Email Manager 审计日志导出选项

要导出 Personal Email Manager 审计日志记录:

1. 从 **Export range（导出范围）**下拉列表选择时间段（当前页面、最近 24 小时，或最近 3 天）。
2. 单击 **Go（执行）**。

3. 在 **Export Log（导出日志）**对话框中选择所需的输出文件类型。
   - 如果选择 **CSV**，将打开一个对话框，让您以 CSV 格式打开或保存文本文件。
   - 如果选择 **HTML**，将打开一个对话框，让您打开或保存包含日志数据的 HTML 文件。
4. 单击 **OK（确定）**。

系统日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Gateway 的系统日志记录反映系统的当前状态，以及产生的任何错误或警告。单击 **Main（主页）> Status（状态）> Logs（日志）**页面上的 System Log（系统日志）选项卡可查看系统日志，以及可根据需要将所选部分导出为 CSV 或 HTML 文件。

系统日志记录保存期为 30 天。要使系统日志记录保持时间超过 30 天，请定期使用 Export（导出）选项导出日志。导出操作不会从系统日志删除记录。它会将日志数据转换成 CSV 或 HTML 文件。

System Log（系统日志）页面打开时，会显示最近的记录。使用日志上方的 **View（查看）**下拉列表选项选择要查看的日志条目范围：All（所有）、One Day（一天）、One Week（一周）、One Month（一个月）或 Custom（自定义）。选择 **Custom（自定义）**时，使用 **View from/to（查看自 / 至）**字段可指定要查看的日志条目的所需日期 / 时间范围。日历包括以下选项:

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。

也可以在视图的类型下拉列表中选择事件类型，按系统事件类型查看日志条目。

在 View（查看）选项下面，从 **Per page（每页）**下拉列表中选择希望每个日志页面显示的日志条目数（25 至 200）。默认值为 25。在页面顶部和底部，使用上一页或下一页箭头可滚动显示日志，也可以在 **Page（页面）**字段中输入要查看的页面并单击 **Go（进入）**。

系统日志数据

日志显示以下信息:

列	说明
Date（日期）	系统事件的日期和时间（根据时区而调整）。 为确保系统日志中数据的一致性，请确保运行 Websense 组件的机器的日期和时间设置是同步的。
Server（服务器）	受系统事件影响的机器 IP 地址
Type（类型）	系统事件类型（更新、配置异常、混合模式、集群、日志、隔离、扫描引擎、DLP、补丁和 hotfix、看门狗、系统维护或警报）
Message（消息）	用于打开 Details（详细信息）消息框的链接，消息框中显示系统事件的相关信息

系统日志导出选项

要导出系统日志记录:

1. 从 **Export range（导出范围）**下拉列表选择时间段（当前页面、最近 24 小时、最近 7 天或最近 30 天）。

   选择 **Last 30 days（最近 30 天）**导出整个系统日志文件。
2. 单击 **Go（执行）**。
3. 在 **Export Log（导出日志）**对话框中选择所需的输出文件类型。
   - 如果选择 **CSV**，将打开一个对话框，让您以 CSV 格式打开或保存文本文件。
   - 如果选择 **HTML**，将打开一个对话框，让您打开或保存包含日志数据的 HTML 文件。
4. 单击 **OK（确定）**。

控制台日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

控制台日志记录任何管理员在 TRITON Unified Security Center 的 Email Security 模块上执行的活动或更改。单击 **Main（主页）> Status（状态）> Logs（日志）**页面的 Console Log（控制台日志）选项卡可查看控制台日志，以及根据需要将所选部分导出为 CSV 或 HTML 文件。

控制台日志记录在数据库中保存的时间长度取决于数据库分区容量。要保存控制台日志记录，请定期使用 Export（导出）选项导出日志。导出操作不会从控制台日志删除记录。它会将日志数据转换成 CSV 或 HTML 文件。

Console Log（控制台日志）页面打开时，会显示最近的记录。使用日志上方的 **View（查看）**下拉列表选项选择要查看的日志条目范围：All（所有）、One Day（一天）、One Week（一周）、One Month（一个月）或 Custom（自定义）。选择 **Custom（自定义）**时，使用 **View from/to（查看自 / 至）**字段可指定要查看的日志条目的所需日期 / 时间范围。日历包括以下选项：

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。

在 View（查看）选项下面，从 **Per page（每页）**下拉列表中选择希望每个日志页面显示的日志条目数（25 至 200）。默认值为 25。在页面顶部和底部，使用上一页或下一页箭头可滚动显示日志，也可以在 **Page（页面）**字段中输入要查看的页面并单击 **Go（进入）**。

控制台日志数据

日志显示以下信息：

列	说明
Date（日期）	更改的日期和时间（根据时区而调整）。 为确保控制台日志中数据的一致性，请确保运行 Websense 组件的机器的日期和时间设置是同步的。
User（用户）	做出更改的管理员用户名
Client（客户端）	进行更改的管理员机器的 IP 地址
Role（角色）	做出更改的管理员角色，本例中为超级管理员
Action（操作）	更改的类型（例如指示管理员登录或注销、管理员角色变化或添加新用户的条目）
Action Detail（操作详细信息）	用于打开 Details（详细信息）消息框的链接，消息框中显示所做更改的相关信息

控制台日志导出选项

要导出控制台日志记录：

1. 从 **Export range（导出范围）**下拉列表选择时间段（当前页面、最近 24 小时、最近 7 天或最近 30 天）。

   选择 **Last 30 days（最近 30 天）**导出整个控制台日志文件。
2. 单击 **Go（执行）**。

3. 在 **Export Log（导出日志）**对话框中选择所需的输出文件类型。
   - 如果选择 **CSV**，将打开一个对话框，让您以 CSV 格式打开或保存文本文件。
   - 如果选择 **HTML**，将打开一个对话框，让您打开或保存包含日志数据的 HTML 文件。
4. 单击 **OK（确定）**。

混合服务日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

混合服务日志包含在到达网络之前被混合服务阻止的电子邮件记录。要使混合服务日志可用，必须已输入有效的 Email Security Gateway Anywhere 订购序列号并成功地注册 Email Security 混合服务（有关详细信息，请参阅注册混合服务（第 35 页））。

注册 Email Security 混合服务后，可以在 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Service Log Options（混合服务日志选项）**页面中启用混合服务日志和设置数据传送选项。有关信息，请参阅配置混合服务日志（第 40 页）。

在 **Main（主页）> Status（状态）> Logs（日志）**页面单击 Hybrid Service（混合服务）选项卡访问混合服务日志。

在日志表格横幅中的 **Per page（每页）**下拉列表中可以配置每个日志页面的日志条目数（25-200，默认值为 25）。在页面顶部和底部，按上一页或下一页箭头可滚动显示混合服务日志的页面，也可以在 **Page（页面）**字段中输入具体的页码并单击 **Go（进入）**。

邮件记录在数据库中保存的时间长度取决于邮件数量和数据库分区容量。要保存邮件记录，请定期使用 Export（导出）选项导出日志内容。导出操作不会从混合服务日志删除记录。它会将日志数据复制到 CSV 或 HTML 文件。

Hybrid Service Log（混合服务日志）页面出现时，会显示最近的记录。使用 **View from/to（查看从 / 至）**字段可指定要查看的日志条目的日期 / 时间范围。日历包括以下选项:

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。

混合服务日志数据

将收集以下邮件数据并以表格形式显示:

邮件数据项目	说明
Hybrid Service Log ID（混合服务日志 ID）	数据库生成的邮件标识符
Date/Time（日期 / 时间）	接收邮件的日期和时间
Subject（主题）	邮件主题
Sender Address（发件人地址）	发件人电子邮件地址
Recipient Address（收件人地址）	收件人电子邮件地址。如果邮件有多个收件人，则显示第一个收件人地址。
Sender IP（发件人 IP）	邮件发件人 IP 地址
Message Status（邮件状态）	当前邮件状态（例如已丢弃或退回）
Reason（原因）	由混合服务提供，确定邮件处理方式的扫描结果

混合服务日志搜索选项

混合服务日志包含多个搜索选项，包括日期范围或关键字搜索。在 **View from/to（查看自 / 至）**字段日历控件中选择日期，以确定搜索的日期 / 时间范围。**from（自）**或 **to（至）**字段的默认值是您打开日志的日期和时间。

进行关键字搜索时，可从 **Keyword search（关键字搜索）**下拉列表中选择要搜索的日志元素，然后在列表右边的字段中输入搜索词。单击 **Search（搜索）**启动搜索功能。

在所有混合服务日志元素中搜索关键字，或在下列任一混合服务日志组件中搜索:

- Hybrid Service Log ID（混合服务日志 ID）
- Subject（主题）
- Sender Address（发件人地址）
- Recipient Address（收件人地址）
- Sender IP（发件人 IP）
- Message Status（邮件状态）

单击 **Set to Default（设置为默认）**将关键字搜索选项恢复为默认设置（所有混合服务日志组件和关键字字段为空白）。

混合服务日志导出选项

要导出混合服务日志搜索结果:

1. 单击 **Export（导出）**打开 Export Log（导出日志）对话框。
2. 选择所需的输出文件类型（CSV 或 HTML）。
   - 如果选择 **CSV**，将打开一个对话框，让您以 CSV 格式打开或保存文本文件。
   - 如果选择 **HTML**，将打开一个对话框，让您打开或保存包含日志数据的 HTML 文件。
3. 选择要导出的页面（所有页面、当前页面或页面范围）。
4. 单击 **OK（确定）**。

Real-time monitor

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

可以在所选设备的 **Main（主页）> Status（状态）> Real-Time Monitor** 页面上，查看电子邮件流量的实时日志信息。在进行故障排除时此信息会很有用。

勾选相应的复选框，指定以下任一或所有类型的日志信息用于显示:

- Message status（邮件状态）（默认设置）
- Connection status（连接状态）
- Message delivery status（邮件传送状态）
- Message analysis result（邮件分析结果）

默认情况下会监控当前设备。要在集群模式下监控多台设备，请单击 **Select（选择）**，然后在 **Select Appliance（选择设备）**列表中勾选适当的复选框。确保选中主要集群设备。

当用户打开 Real-Time Monitor 屏幕时，监控器会自动启动。可使用以下按钮控制监控器运行时间:

Pause（暂停），暂时停止实时日志流

Start（开始），打开指定设备电子邮件流量数据的运行日志

在 **Search filter（搜索过滤器）**字段中输入搜索词，执行单个日志条目的关键字搜索。

单击 **Advanced Search（高级搜索）**，打开其他过滤器选项。您可以搜索日志条目并按邮件主题、IP 地址（来源、目的地或两者皆选）或电子邮件地址（发件人、收件人或两者皆选）显示记录。

安全信息和事件管理 (SIEM) 集成

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

通过第三方安全信息和事件管理 (SIEM) 工具可以记录和分析网络设备和软件生成的内部警报。通过集成 SIEM 技术，Email Security Gateway 可以将邮件活动事件传送至 SIEM 服务器进行分析和报告。

在 **Settings（设置）> General（一般）> SIEM Integration（SIEM 集成）**页面上访问 SIEM 集成设置。勾选 **Enable SIEM integration for all Email Security Gateway appliances（为所有 Email Security Gateway 设备启用 SIEM 集成）**复选框可激活 SIEM 集成功能。

启用 SIEM 集成后，使用下列步骤配置 SIEM 服务器和传输协议:

1. 在 **IP address or host name（IP 地址或主机名称）**输入字段中输入 SIEM 集成服务器的 IP 地址或主机名称。
2. 在 **Port（端口）**字段中输入 SIEM 集成服务器的端口号。默认值为 514。
3. 选择用于数据传输的协议（**UDP** 或 **TCP**）。用户数据报协议 (UDP) 是 Internet 协议套件中的传输层协议。UDP 无状态，因此速度比传输控制协议 (TCP) 快，但可能不可靠。与 UDP 类似，TCP 也是传输层协议，但它可以传输速度为代价，提供可靠的有序数据发送。
4. 单击 **Send Test Message（发送测试邮件）**，确认已正确配置 SIEM 产品并可以从 Email Security Gateway 接收邮件。

混合服务配置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Websense Email Security Gateway Anywhere 提供灵活而全面的电子邮件安全解决方案，可让您根据需要结合本地和混合（云）过滤来管理组织的入站和出站电子邮件。

混合服务提供额外的层来扫描电子邮件，阻止垃圾邮件、病毒、仿冒及其它恶意攻击进入网络，可显著节省电子邮件带宽和存储空间。您也可以使用混合服务在出站电子邮件发送至收件人之前对其加密。

通过 Email Security Gateway Anywhere，您可以在同一用户界面 Email Security 管理器中创建本地及混合过滤策略，并集中进行配置、报告和管理。

在使用混合服务过滤组织的电子邮件之前，必须通过在 Email Security 管理器和域名系统 (DNS) 中输入有效的 Email Security Gateway Anywhere 订购密钥和配置一系列设置来激活混合帐户。这将在 Email Security Gateway Anywhere 的本地与混合部分之间建立连接。有关详细信息，请参阅注册混合服务（第 35 页）。

混合服务日志包含在到达网络之前被混合服务阻止的电子邮件记录。有关该日志内容的信息，请参阅混合服务日志（第 31 页）。有关启用和安排混合服务日志更新的详细信息，请参阅配置混合服务日志（第 40 页）。

注册混合服务

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

选择 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**以激活混合帐户。单击 **Register（注册）**后，注册向导将会打开。按照下列步骤在向导页面中操作:

1. 输入用户信息（第 36 页）
2. 指定传送路由（第 37 页）
3. 配置 *DNS*（第 38 页）
4. 设置防火墙（第 39 页）
5. 配置 *MX* 记录（第 39 页）
6. 修改混合服务配置（第 40 页）

重要事项

单一 Email Security Gateway 管理器控制的多个设备，无论采取何种设备模式（集群或独立），都共享相同的混合服务配置设置。

如果需要在同一个 Email Security 管理器上注册多个采用混合服务的设备，应该:

1. 将所有设备添加至 Email Security Gateway 管理器（**Settings（设置）> General（一般）> Email Appliances（电子邮件设备）**）。
2. 创建设备集群（**Settings（设置）> General（一般）> Cluster Mode（集群模式）**）。
3. 输入 Email Security Gateway Anywhere 订购序列号（**Settings（设置）> General（一般）> Subscription（订购）**）。
4. 注册混合服务（**Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**）。如果您的设备以独立模式运行，请从输入了订购序列号的设备注册。

注册混合服务后，可能需要添加设备（例如购买新设备后）。在这种情况下，应该将新设备添加至 Email Security Gateway 管理器，然后再次注册现有混合服务设备，而无需改变任何配置设置。再次注册后，所有设备的混合服务配置都会同步。

输入用户信息

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**的 Basic Information（基本信息）页面中提供 Websense 过滤管理员的联系人电子邮件地址、电话号码以及所在国家。

电子邮件地址通常为负责管理 Websense 软件的团队所监控的别名。发送至您帐户的这封邮件非常重要，应在收到后立即激活。

- Websense 技术支持使用此地址发送影响混合过滤的紧急情况通知。
- 如果您的帐户配置有问题，未能及时回复技术支持发出的电子邮件可能会导致服务中断。
- 如果出现异常情况，此电子邮件地址可用于发送允许同步服务恢复与混合服务的联系的信息。
- 此电子邮件地址**不**用于发送营销、销售或其它一般信息。

您输入的国家名称将为系统提供时区信息。

单击 **Next（下一步）**继续混合配置。

指定传送路由

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**下的 Delivery Route（传送路由）页面，可以指定电子邮件与混合服务通信的域以及混合服务收发邮件的 SMTP 服务器地址。每组域和 SMTP 服务器地址都包含传送路由。

重要事项

混合服务检查通过向“邮件管理员”地址发送命令来检查到 SMTP 服务器的连接。如果 SMTP 服务器没有邮件管理员或管理员地址（例如 postmaster@mydomain.com），则应该手动添加该地址以完成此步骤。

要添加传送路由:

1. 在 Delivery Route（传送路由）页面中单击 **Add（添加）**。
2. 输入 **Delivery route name（传送路由名称）**。
3. 要添加域到传送路由，在 Protected Domains（受保护的域）下单击 **Add（添加）**。
4. 输入 **Domain Address（域地址）**（例如 mydomain.com）。
5. 指定传送路由是否应该用于该域的所有子域。
6. 要添加其它域，请重复步骤 3-5。

注

此处添加的受保护域必须已经输入到 **Settings（设置）> Users（用户）> Domain Groups（域组）**页面的 Protected Domains（受保护的域）组中。有关信息，请参阅管理域和 *IP* 地址组（第 58 页）。

7. 要添加入站 SMTP 服务器到传送路由，请单击 SMTP Inbound Server Addresses（SMTP 入站服务器地址）下的 **Add（添加）**。
8. 输入 Email Security Gateway 服务器的 IP 地址或名称。必须输入从外部网络可以看到的外部 IP 地址或名称。

   要添加更多服务器，请再次单击 **Add（添加）**。每个新增的服务器都将获得下一个可用的 ID 号，并且被添加至列表底部。最小的 ID 号具有最高的优先顺序。邮件始终被享有最高优先顺序的服务器接收；如果此服务器无法接收，则由传送路由中次高优先顺序的服务器接收。

   要更改优先顺序，请勾选服务器名称旁边的复选框，然后单击 **Move up（上移）**或 **Move down（下移）**。

9. 要添加出站 SMTP 服务器到传送路由，请单击 SMTP Outbound Server Addresses（SMTP 出站服务器地址）下的 **Add（添加）**。Email Security Gateway 使用这些 IP 地址发送电子邮件到混合服务进行加密。有关此加密功能的信息，请参阅高级电子邮件加密（第 108 页）。
10. 输入 Email Security Gateway 服务器的 IP 地址或名称。必须输入从外部网络可以看到的外部 IP 地址或名称。

    要添加更多服务器，请再次单击 **Add（添加）**。每个新增的服务器将会添加到列表底部。如果出站服务器连接失败，此条传送路由中需要加密的电子邮件将发送至延迟邮件队列，稍后再发送。
11. 单击 **OK（确定）**。

    传送路由显示于 Delivery Route（传送路由）页面的 Route List（路径列表）中。

单击 **Next（下一步）**继续混合配置。

配置 DNS

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

按照 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**下的 CNAME Records（CNAME 记录）页面中的信息配置 DNS。

传送路由被混合服务接受之前，必须先通过检查，以确保服务能够发送每个受保护域的邮件到邮件服务器，并且每个域都属于您的企业。

CNAME 记录用于分配别名到 DNS 中的现有主机。请联系您的 DNS 管理机构（通常是您的 Internet 服务提供商），请求他们使用 DNS 页面上的别名和相关域信息为您的每个受保护域创建 CNAME 记录。

CNAME 记录采用以下格式:

```
abcdefgh.mydomain.com CNAME autodomain.mailcontrol.com.
```

其中:

- `abcdefgh` 是显示在 DNS 页面上的 **Alias（别名）**
- `mydomain.com` 是 **Protected Domain（受保护的域）**
- `CNAME` 表示您在指定 CNAME 记录
- `autodomain.mailcontrol.com` 是与上述别名及受保护域一起显示的 **Associated domain（相关域）**

请确保相关域名中含有尾随句点 "."。

以上示例表明，别名 **abcdefgh.mydomain.com** 已分配到 **autodomain.mailcontrol.com**。这便于混合服务确认您拥有 **mydomain.com**。

创建 CNAME 记录后，单击 **Check Status（检查状态）**以验证您的条目是否已在 DNS 中正确设置。如果有必要的话，解决任何错误状况。如果页面上没有显示 **Check Status（检查状态）**按钮，只需单击 **Next（下一步）**继续操作即可。

> **注**
> 通过单击 **Check Status（检查状态）**执行的验证发生在本地系统中。在所有 Internet 服务器之间传播 DNS 更改可能需要几分钟到几小时的时间，因此混合服务的验证过程可能需要更长时间。

单击 **Next（下一步）**继续混合配置。

设置防火墙

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

按照 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**下的 Network Access（网络访问）页面中的信息配置防火墙。

因为混合服务是一项托管服务，因此由 Websense 负责管理系统容量。有鉴于此，电子邮件的路线在混合服务中有时可能会改变。为了让此改变无缝发生而无需您做出进一步改动，必须允许来自 Network Access（网络访问）页面中所有 IP 范围的 SMTP 访问请求传送到 Email Security Gateway 端口 25。

单击 **Next（下一步）**继续混合配置。

配置 MX 记录

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

按照 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**下的 MX Records（MX 记录）页面中的信息配置 Mail eXchange (MX) 记录。

MX 记录是 DNS 数据库中定义将要接受指定机器邮件的主机的条目。MX 记录必须通过混合服务将入站电子邮件路由到 Email Security Gateway。

以 **in.mailcontrol.com** 结尾的 MX 记录列在 MX Records（MX 记录）页面上。请联系您的 DNS 管理机构（通常是您的 Internet 服务提供商），请求他们使用 MX Records（MX 记录）页面上的混合服务所提供的客户特定记录，为您指定的每个受保护域创建或替换当前 MX 记录。例如，他们可能更改:

更改	自	至
MX Preference 1（MX 优先顺序 1）	mydomain.com. IN MX 50 mail.mydomain.com.	mydomain.com. IN MX 5 **cust0000-1.in.mailcontrol.com**.
MX Preference 2（MX 优先顺序 2）	mydomain.com. IN MX 51 mail.mydomain.com.	mydomain.com. IN MX 5 **cust0000-2.in.mailcontrol.com**.

确保它们包含尾随句点，并且要求他们将每条记录设置为相等的优先顺序值。

检查 Internet 服务提供商 DNS 管理站点上的条目，以确保它们与混合服务所提供的 MX 记录相符。验证条目后，单击 **Check Status（检查状态）**以确认更新是否成功。

将 MX 记录中的更改全部传播到 Internet 可能需要长达 24 小时。在此期间，应保持原邮件路由为活动状态，以确保所有邮件都能送达。在 MX 记录更改完成时，有些邮件仍然使用原 MX 信息传送，有些邮件则使用新的 MX 信息传送。

单击 **Finish（完成）**完成混合配置。

修改混合服务配置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

完成注册向导后，您可以在 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**编辑页面中检查和修改混合服务配置设置。

> **注**
> 如果混合服务已经验证域所有权，CNAME records（CNAME 记录）区可能不会显示 **Check Status（检查状态）**按钮。

应该通过从受保护的域以外发送电子邮件到 Email Security Gateway，来确保已通过混合服务正确地路由电子邮件。

配置混合服务日志

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

混合服务日志选项在 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Service Log Options（混合服务日志选项）**页面上设置。可以在此页面上启用混合服务日志并确定日志的数据传输计划。

这些选项仅在已经输入有效的 Email Security Gateway Anywhere 订购序列号并已经注册 Email Security 混合服务的情况下可用。

按照以下步骤配置混合服务日志选项:

1. 通过勾选 **Enable the Hybrid Service Log（启用混合服务日志）**复选框启用混合服务日志。
2. 在 **Retrieve Hybrid Service Log data every（检索混合服务日志数据的频度）**下拉框中，指定检索最新混合服务日志信息的时间间隔（15 分钟至 24 小时）。默认值为 15 分钟。
3. 在 **Send the Hybrid Service Log data to the database every（向数据库发送混合服务日志数据的频度）**下拉框中，指定向日志数据库发送混合服务日志信息的时间间隔（15 分钟至 24 小时）。默认值为 15 分钟。
4. 单击 **OK（确定）**。

向 Websense Data Security 注册

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以通过在 **Main（主页）> Policy Management（策略管理）> Policies（策略）**页面中启用 Data Security 电子邮件策略，允许 Email Security Gateway 分析电子邮件的合规性和适用性以及防止通过电子邮件泄露敏感数据。Data Security 策略默认启用。有关激活数据泄露防护策略的详细信息，请参阅*启用 Data Security 策略*（第 127 页）。

可在 TRITON Unified Security Center 的 Data Security 模块中（**Main（主页）> Policy Management（策略管理）> DLP Policies（DLP 策略）> Manage Policies（管理策略）**）配置 Data Security 电子邮件数据泄露防护策略选项。一个新的策略向导提供了创建新的 Data Security 电子邮件 DLP 策略的相关步骤。有关详细信息，请参阅 *Data Security 管理器帮助*。

如果您计划使用电子邮件加密功能，则必须使用包括邮件加密的操作计划配置 Data Security 策略。有关详细信息，请参阅 *Data Security 管理器帮助*。

还可以在 Email Security Gateway 中创建过滤器操作以用于 Data Security 操作计划。有关配置 Data Security 过滤器操作的信息，请参阅创建和配置过滤器操作（第 122 页）。

必须向 Data Security 管理器注册 Email Security Gateway 设备，才可利用其适用性、数据泄露防护和邮件加密功能。在输入有效的 Email Security Gateway 订购序列号时会自动进行注册。从 Email Security 管理界面添加后续设备到 TRITON Unified Security Center 时，将会注册这些设备。

如果 Email Security 的 **Settings（设置）> General（一般）> Data Security（数据安全）**页面中的 Status（状态字段）显示 **Unregistered（未注册）**，则必须手动向 Data Security 注册。

在 Email Security 的 **Settings（设置）> General（一般）> Data Security（数据安全）**页面中使用下列步骤向 Data Security 管理器注册独立设备:

1. 在 **Settings（设置）> General（一般）> Subscription（订购）**页面中输入有效的 Email Security Gateway 订购序列号。
2. 在 **Communication IP address（通信 IP 地址）**下拉列表中指定用于与 Email Security Gateway 通信的 IP 地址。

   注
   默认将选择设备 C 接口 IP 地址。Data Security 注册建议使用该设置。

3. 选择 **Manual（手动）**注册方式以启用 Properties（属性）输入字段。

4. 指定下列 Data Security 服务器属性:
   - IP address（IP 地址）
   - User name（用户名）
   - Password（密码）
5. 单击 **Register（注册）**。
6. 必须在 Data Security 模块中部署 Data Security 策略以完成整个过程。单击 Data Security 模块选项卡，然后单击 **Deploy（部署）**。

> **重要事项**
> 应等待 Data Security 策略部署完成后再注册另一个独立设备。

如果在设备集群中部署 Email Security Gateway，要注意以下问题:

- 在 Data Security 中部署数据泄露防护策略之前，向 Data Security 注册所有主要和次要机器。如果在主要设备上部署 Data Security 策略的同时向 Data Security 注册次要机器，则次要机器的注册过程可能无法完成。
- 确保集群中的所有机器使用同一个物理设备接口（C、E1 或 E2 IP 地址）向 Data Security 注册。

电子邮件过滤数据库更新

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

定期更新电子邮件过滤数据库可最大程度地防范电子邮件附带的攻击。使用 **Settings（设置）> General（一般）> Database Downloads（数据库下载）**页面，可管理防垃圾邮件和防病毒过滤数据库的更新。

防病毒和防垃圾邮件过滤表格列出了 Email Security 订购所包含的过滤数据库集。如果当前设备为主要机器，这些表格同时包含与主要机器关联的任何次要机器的更新信息。第一次下载数据库时，每个过滤器的默认更新时间表为每小时一次。

要编辑单个过滤器的更新时间表，请单击要更改的数据库旁边的 **Edit（编辑）**。在 Reschedule Filter Update（重新计划过滤器更新）对话框中，按需要配置以下设置:

频率	您希望更新的频率（从每 15 分钟一次到每周一次）
Day of week（星期几）	此字段仅在频率选择为 **Every week（每周）**时才可用。选择在星期几更新。
Time（时间）	此字段仅在频率选择为 **Every day（每天）**或 **Every week（每周）**时才可用。选择每日更新的时间。

使用 **Update Now（立即更新）**立即更新所有 Websense 数据库。

使用 Web Security 的 URL 扫描

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Gateway 使用 Websense Web Security URL 扫描进行准确而高效的垃圾邮件检测。Web Security 模块会从 Websense 下载服务器维持最新的 URL 主数据库。Email Security Gateway 会查询 Websense URL 类别主数据库并确定邮件中发现的 URL 的风险级别。请注意，Web Security 版本必须为 Email Security Gateway 所支持，此功能才可用。

在 **Settings（设置）> General（一般）> URL Scanning（URL 扫描）**页面中指定主数据库的位置:

- 如果 Web Security 和 Email Security 安装于同一台 Websense V-Series™（V 系列）设备上，请使用 **Local（本地）**选项。
- 使用 **Remote（远程）**选项，以便使用远程数据库。输入远程数据库的 IP 地址或主机名。

在 **Main（主页）> Policy Management（策略管理）> Filters（过滤器）> Add URL Scanning Filter（添加 URL 扫描过滤器）**页面中，通过勾选 Filter Properties（过滤器属性）部分的 **URL scanning（URL 扫描）**复选框并选择想要 Email Security 扫描的 URL 类别，激活 URL 扫描。有关详细信息，请参阅 *URL 扫描*（第 115 页）。

使用代理服务器

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以为电子邮件过滤数据库更新或混合服务与 Internet 之间的电子邮件流量配置代理服务器。请注意，您可以使用同一个代理服务器来执行这两项功能。

如果使用代理服务器进行数据库更新，请勾选 **Enable filtering database update proxy server（启用过滤数据库更新代理服务器）**复选框。如果使用代理服务器进行混合服务通信，请勾选 **Enable hybrid service proxy server（启用混合服务代理服务器）**复选框。

注

Email Security Gateway 不支持使用安全套接字层 (SSL) 代理进行过滤数据库更新。SSL 服务器可用作混合服务代理。

如果在同一个 Websense V 系列设备（V10000 G2 或 V10000 G3）上运行 Email Security Gateway 和 Websense Web Security Gateway，可以将 Web Security Gateway 设为代理服务器。

使用 **Settings（设置）> General（一般）> Proxy Server（代理服务器）**页面输入以下代理服务器信息:

1. 在 **Server IP address or host name（服务器 IP 地址或主机名称）**字段中输入代理服务器的 IP 地址或主机名称。
2. 在 **Port（端口）**字段中输入代理服务器的端口号。
3. 在 **User name（用户名）**和 **Password（密码）**字段中输入代理服务器的用户名和密码。

使用 Common Tasks（常见任务）窗格

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

右侧的 Common Tasks（常见任务）快捷方式窗格为经常执行的管理任务（例如运行报表、创建策略或搜索日志）提供快捷方式。单击列表中的项目可跳转到用于执行该任务的页面。

3 配置系统设置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

主题:

管理管理员帐户

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Gateway 管理员帐户在 TRITON Unified Security Center 的 Administrators（管理员）页面中创建。仅超级管理员可以在 TRITON Settings（TRITON 设置）页面中添加、编辑或删除管理员帐户。在模块区中单击 **TRITON Settings（TRITON 设置）**可访问 **TRITON Settings（TRITON 设置）> Administrators（管理员）**页面。

超级管理员可以创建两类帐户：本地和网络。本地帐户存储在本地 TRITON Unified Security Center 数据库中，只包含一个用户。网络帐户可以包含一个用户或一组用户，存储在网络服务器中。有关在此页面上管理 TRITON 控制台管理员的详细信息，请参阅 *TRITON Unified Security Center* 帮助。

在一台设备上配置的管理员帐户设置和角色分配会应用于您网络中的所有设备。

管理员帐户

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Settings（设置）> Administrators（管理员）> Delegated Administrators（委托管理员）页面列出所有已定义的 Email Security 管理员、他们的电子邮件地址、帐户类型、角色，以及管理员的当前状态（联机或脱机）。

会创建一名新的 Email Security 管理员，角色为审计员。Email Security 超级管理员可以将默认角色分配给新建的管理员帐户，或为该管理员新建一个角色。单击管理员名称可打开 Edit Administrator（编辑管理员）页面。

在 **Role（角色）**下拉列表中选择管理员，可将该管理员指派给默认角色。如果想要为该管理员创建一个拥有不同权限的新角色，也可以单击 **New Role（新建角色）**。有关添加新角色和定义权限的信息，请参阅管理员角色（第 47 页）。

可以选择以下默认角色:

默认角色	说明
Super Administrator（超级管理员）	此角色的管理员拥有充分的访问权限。他们可以添加和移除管理员，并可编辑所有其他管理员的个人资料和权限。
Auditor（审计员）	此角色的管理员可以查看所有配置设置，但无法进行更改。
Reporting Administrator（报表管理员）	此角色的管理员仅可以编辑、运行和计划报表。
Security Administrator（安全管理员）	此角色的管理员可以访问所有常规设置，并可以添加域、设置路由和首选项。除了不能管理其他管理员，其他权限与超级管理员相同。
Policy Administrator（策略管理员）	此角色的管理员仅可以为该角色所管理的特定用户或群组创建和管理策略。其权限包括为该等用户和群组执行报告和隔离管理。
Quarantine Administrator（隔离管理员）	此角色的管理员可以管理特定队列、依据日志排查故障，以及从分配的队列中解除对邮件的阻止并传送给用户。
Group Reporting Administrator（群组报表管理员）	此角色的管理员仅可以为特定群组中的用户编辑、运行和计划报表。

在 Edit Administrator（编辑管理员）页面上单击 **View Permission（查看权限）**可看到一个只读屏幕，其中显示该管理员的当前角色和权限。

管理员角色

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Gateway 允许超级管理员创建若干个委托管理员并为其指定各种角色和权限。当为 Email Security Gateway 委托管理员创建新角色时，需指定该角色管理的用户或群组，并指定角色的权限。然后，为该角色分配管理员。一次仅可将一名管理员分配给一个角色。

注

所管理的用户和用户组设置仅可用于以下权限:

- 策略
- 报表
- 队列和隔离邮件

用户的 Email Security Gateway 管理器界面的视图因该用户的特定管理员角色而有所不同。例如，角色为“审计员”的用户可以查看整个 Email Security 管理器界面，但该用户无法修改任何设置。

默认情况下，新的 Email Security 特定模块管理员帐户为审计员帐户。超级管理员可以使用下列步骤更改管理员角色:

注

每次只允许一位超级管理员访问 Email Security Gateway 设备。随后的超级管理员在访问设备时将被分配审计员（或只读）角色。

添加角色

单击 **Add（添加）**并使用以下步骤创建新的管理员角色:

1. 输入新角色的名称，以及对该角色的简短、清晰的描述。
2. 定义要让该角色管理的用户或用户组:
   a. 在 Managed Users and Groups（所管理的用户和群组）表格下方单击 **Add（添加）**，打开 Add Managed Users and Groups（添加管理的用户和群组）对话框。
   b. 以下列其中一种方式输入所管理的用户和群组的电子邮件地址:
      - 浏览至一个电子邮件地址文件夹 — 每行包含一个电子邮件地址并且小于 10 MB 的文本文件。
      - 在用户电子邮件地址框中输入所需的电子邮件地址，用英文分号分隔。

3. 在 Permissions（权限）表中为该角色定义权限。提供了下列选项:

模块	权限选项
策略	Read-only access to all policies （以只读方式访问所有策略） Management（管理） Policies for users managed by this role （该角色所管理用户的策略） All policies（所有策略）
系统设置和状态（包括访问 System Log（系统日志）、Alerts（警报）页面、Message Queues（邮件队列）页面以及 Settings（设置）选项卡上除 Administrators（管理员）外的所有菜单项目）	None（无） Read-only access（只读访问权限） Management（管理）
Real-Time Monitor	None（无） Read-only access（只读访问权限）
邮件日志（包括访问 Message（邮件）、Connection（连接）和 Hybrid Service（混合服务）日志）	None（无） Read-only access to all message logs （以只读方式访问所有邮件日志） Manage message logs for users managed by this role （管理该角色所管理用户的邮件日志） Manage all message logs（管理所有邮件日志）
审计和控制台日志（包括访问 Audit（审计）、Console（控制台）和 Personal Email Manager 日志）	None（无） Access to logs（访问日志）
管理员	None（无） Read-only access（只读访问权限） Management（管理）
报表	None（无） Reports for users managed by this role （该角色所管理用户的报表） Access to all reports（访问所有报表）
队列和隔离邮件	队列访问（None（无）、Access to all queues（访问所有队列）、Access to selected queue（访问所选队列）） Manage all quarantined messages（管理所有隔离邮件） Manage messages for users managed by this role （管理该角色所管理用户的邮件） Read-only access to all quarantined messages （以只读方式访问所有隔离邮件）

4. 单击 **Assign Role（分配角色）**打开 Assign Role（分配角色）对话框。
5. 选择要为其分配该角色的管理员。该角色会替换管理员的当前角色。
6. 单击 **OK（确定）**。

设置系统首选项

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

可以在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面中完成以下 Email Security 系统首选项:

- 输入全限定域名
- 设置 *SMTP* 问候
- 设置系统通知电子邮件地址
- 配置管理员控制台首选项

输入全限定域名

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

SMTP 协议要求使用全限定域名 (FQDN) 来传输邮件。如果完成首次配置向导，则在向导中输入的 FQDN 会作为默认条目出现在该页面上。

如果未完成向导，则在 **Fully Qualified Domain Name（全限定域名）**字段中输入设备的全限定域名（格式为 appliancehostname.parentdomain.com）。

重要事项

该设置对于 Email Security Gateway 的正常工作非常重要。必须将默认的全限定域名条目替换为正确的设备名称。

错误的全限定域名可能导致电子邮件流量中断。

设置 SMTP 问候

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

SMTP 问候是对远程服务器连接尝试的响应，还可用于指示系统能否正确运作。例如，默认 SMTP 问候为

```
Websense Email Security Gateway Service is ready
（Websense Email Security Gateway 服务已就绪）。
```

在 **SMTP greeting（SMTP 问候）**字段中输入文本可更改默认问候。

设置系统通知电子邮件地址

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security 可自动发送系统事件通知（例如已停止的服务）到预定义的地址（通常是管理员地址）。在 **Administrator email address（管理员电子邮件地址）**字段中输入所需的收件人地址。

如果需要管理员电子邮件地址收发系统事件以外的通知邮件，必须同时在此字段中输入地址。例如，要配置管理员地址在邮件触发过滤器时收发通知（在 **Main（主页）> Policy Management（策略管理）> Actions（操作）**），要求 System Settings（系统设置）页面中的此字段包含管理员地址。

用户通知邮件可发自预定义的地址。在 **Default sender email address（默认发件人电子邮件地址）**字段中输入所需的发件人地址。

配置管理员控制台首选项

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Administrator Console Preferences（管理员控制台首选项）部分可让您配置所需的字符集编码和控制台语言。

从 **Preferred character encoding（首选字符编码）**下拉列表中选择用于对邮件编码的字符集。首选的字符编码设置用于对电子邮件附件解码，包括没有字符编码信息的邮件。

在 **Administrator console language（管理员控制台语言）**下拉列表中设置设备要使用的语言。

管理设备

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在将设备加入 Email Security Gateway 管理平台之前，您应该已经在设备上执行 Websense® V-Series™（V 系列）设备 firstboot 脚本来激活 Email Security 功能，并且在 V 系列 Appliance Manager 中配置了 Email Security 网络接口。接口信息包括 IP 地址、子网掩码、默认网关以及最多 3 个 DNS 服务器 IP 地址。有关详细信息，请参阅 Websense V 系列设备入门指南。

还可以使用 VMware 平台（ESXi v4.0 或更高版本）将 Email Security Gateway 作为虚拟设备进行部署。有关部署和配置 Email Security Gateway 虚拟设备的完整信息，请参阅虚拟设备快速入门指南。

> **注**
>
> Appliance Manager 可用于配置主要、次要及第三 DNS 服务器，其中次要和第三服务器是可选条目。
>
> Email Security Gateway 在启动时会轮询每个 DNS 服务器，确定哪个具有最低延迟等级。无论该服务器在 Appliance Manager 中指定为何，都会被选作 DNS 查询的“主要”服务器。其它服务器可根据主要服务器的网络连接状态用于后续查询。

如果在设备上更改了设备主机名或通信 IP 地址，必须在 Email Security **Settings（设置）> General（一般）> Email Appliances（电子邮件设备）**页面进行同样的更改。Email Security 不会自动检测该等更改。

电子邮件流量通常通过专用的设备接口 (E1/E2) 进行路由。但如果想要通过 C 接口路由流量（例如传输日志数据到 SIEM 服务器），则需要在 V 系列 Appliance Manager 的 **Configuration（配置）> Routing（路由）**页面中定义路由。请注意，每次在设备上添加或删除路由时，都需要停止并重新启动设备上的 Email Security Gateway 服务。

设备概述

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

可以从 **Settings（设置）> General（一般）> Email Appliances（电子邮件设备）**页面管理多个 Email Security 设备，而无需单独登录到每台机器。托管设备共享一个日志数据库，从该数据库生成 Email Security 日志条目、演示报告、仪表盘统计数据和图表。Email Security 管理器和所有设备都必须共享同一个版本和订购序列号，这样设备之间才可顺利通信。

设备可在独立模式（设备加入 Email Security 管理时的默认模式）下操作。也可以将设备指定为主要机器或与主要机器关联的次要机器，以创建设备集群。有关设备集群的更多信息，请参阅指定集群中的主要设备（第 53 页）。

Email Appliances（电子邮件设备）页面以表格列出所有当前系统 Email Security 设备，其中显示设备主机名、平台（V10000 G2、V10000 G3 或 V5000 G2）、系统通信 IP 地址、系统连接状态和模式。它还包含 Action（操作）列，其中的链接可让您切换到独立模式的不同设备（**Launch（启动）**），或者从集群删除未连接的主要设备（**Remove（删除）**）。主要设备被删除后，其所有次要设备将切换到独立模式。此时当前设备以及所有次要设备的 Action（操作）列值都为 **N/A**。

要将 Email Security 设备加入 **Settings（设置）> General（一般）> Email Appliances（电子邮件设备）**页面中的设备列表:

1. 单击 **Add（添加）**。
2. 在 Add Appliance（添加设备）对话框的 **System Communication IP Address（系统通信 IP 地址）**字段中，输入用于与 Email Security Gateway 管理器通信的 IP 地址。
3. 单击 **OK（确定）**。

> **重要事项**
>
> 在 V 系列 Appliance Manager 中更改 Email Security 设备的系统通信 IP 地址会终止与 Email Security Gateway 的连接。要重新建立连接，必须同时在 Email Security 的 **Settings（设置）> General（一般）> Email Appliances（电子邮件设备）**页面中更改 IP 地址。
>
> 此外，还应为 Personal Email Manager 通知邮件（**Settings（设置）> Personal Email（个人电子邮件）> Notification Message（通知邮件）**）更改地址。
>
> 对于 Email Security Gateway Anywhere 的部署，更改了 IP 地址后，必须重新注册混合服务。

添加设备时，会自动向 Data Security 模块注册以获取数据泄露防护。要完成注册过程并部署数据泄露防护策略，请在 TRITON 工具栏中单击 Data Security，然后单击 **Deploy（部署）**。

您可以选择设备并单击 **Delete（删除）**以将该设备从设备列表中删除。请注意，无法删除其他用户正在访问的设备。设备一旦从列表中删除，便无法在 Email Appliances（电子邮件设备）页面对其进行管理。

从设备列表编辑设备设置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以在设备列表中单击设备名称以编辑设备通信 IP 地址。请注意，在此页面中无法更改系统连接状态和模式。

配置设备集群

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Gateway 设备默认以独立模式运行，但可配置为设备集群来管理大量的电子邮件流量。将设备添加到 Email Appliances（电子邮件设备）页面中的设备列表之后，可在 **Settings（设置）> General（一般）> Cluster Mode（集群模式）**页面中从默认的独立模式切换到主要或次要模式。

一些平台限制适用于集群中的设备。无法在有 V5000 G2 设备的集群中配置 V10000 G2 或 V10000 G3 设备。但是，可以将 V10000 G2 设备部署在有 V10000 G3 设备的集群中。一台虚拟设备可与其他虚拟设备集群在一起，但不能与物理设备进行集群。有关详细信息，请参阅 Websense 技术文档库。

集群中的平台版本必须匹配。

集群中的设备上部署的应用程序必须相同。例如，集群中的所有设备都只部署 Email Security，或者除了 Email Security 之外，都还部署有 Websense Web Security。

注

运行 Email Security Gateway 和 Web Security Gateway 的设备不能与运行 Email Security Gateway 和 Web Security 的设备部署在同一个设备集群中。

一个集群中的设备还应具有相同的邮件队列配置。如果在集群创建之前未在主要机器上配置次要设备队列，该队列中的邮件可能会丢失。

重要事项

如果在设备集群中部署 Email Security Gateway 并且要使用 Data Security 策略，请确保先向 Data Security 注册所有主要及次要集群机器，然后在 Data Security 中部署数据泄露防护策略。

如果在主要设备上部署 Data Security 策略的同时向 Data Security 注册次要机器，则次要机器的注册过程可能无法完成。

指定集群中的主要设备

主要设备维护并显示其集群中所有设备的配置设置。请按照下列步骤指定集群中的主要设备:

1. 在 **Settings（设置）> General（一般）> Cluster Mode（集群模式）**页面中，选择 **Cluster (Primary)（集群（主要））**作为设备模式。Cluster Properties（集群属性）对话框将会打开，主要设备 IP 地址显示在 **Cluster communication IP address（集群通信 IP 地址）**字段中。次要设备使用此 IP 地址进行集群通信。

   注

   建议使用 C 设备接口 IP 地址。如果使用该接口，则需要在 V 系列 Appliance Manager 的 **Configuration（配置）> Routing（路由）**页面上定义路由。

   每次在设备上添加或删除路由时，都需要停止并重新启动设备上的 Email Security Gateway 服务。

2. 单击 **Add（添加）**打开 **Add Secondary Appliance（添加次要设备）**页面，在其中可以指定此集群中的次要设备。
3. 从左侧的独立设备列表选择要添加到此集群的次要设备（最多 7 个设备）。

   如果要添加未在列表中的新设备，请单击 **Add New Appliance（添加新设备）**打开 Add Appliance（添加设备）页面。
4. 单击箭头键将设备添加到 Secondary Appliances（次要设备）列表中。
5. 单击 **OK（确定）**。该设备将添加到 Secondary Appliances（次要设备）列表中并显示其状态。
6. 在 Cluster Mode（集群模式）主页面中单击 **OK（确定）**完成设备到集群的添加。

在 Secondary Appliances（次要设备）列表中单击设备名称可打开 Appliance Properties（设备属性）消息框，其中包含有关该设备的所有详细信息。

您可以在 Secondary Appliances（次要设备）列表中选择设备并单击 **Remove（移除）**，将该次要设备从集群中移除。

管理用户目录

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

用户目录是电子邮件过滤的重要组件，用于设置策略的发件人 / 收件人条件。也可提供收件人验证功能以及基本的用户登录身份验证设置。有关用户身份验证设置的信息，请参阅管理用户验证 / 身份验证选项（第 62 页）。

您可以从 **Settings（设置）> Users（用户）> User Directories（用户目录）**页面添加用户目录。

要删除用户目录，可在用户目录列表中选择该目录，然后单击 **Delete（删除）**。仅在 Email Security 未使用该用户目录时才可将其删除。例如，如果该目录用作策略或用户身份验证设置的一部分，则无法删除。

添加和配置用户目录

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 **Settings（设置）> Users（用户）> User Directories（用户目录）**页面中单击 **Add（添加）**可打开 Add User Directory（添加用户目录）页面。指定用户目录的名称后，从下拉列表中选择用户目录类型。请注意，新的用户目录状态为 **Not referenced（未引用）**，因为它尚未被 Email Security 功能使用。用户目录创建条目根据您需要的用户目录类型而有所不同。

按照下列步骤为所需的目录类型创建用户目录:

- *Microsoft Active Directory*
- *IBM LDAP Server Directory*
- *通用 LDAP Server Directory*
- *收件人列表*
- *ESMTP Server Directory*

Microsoft Active Directory

Microsoft Active Directory 在 Windows 环境中提供用户信息管理。请按照下列步骤在 User Directory Properties（用户目录属性）部分配置 Microsoft Active Directory:

1. 在 **Server IP address or host name（服务器 IP 地址或主机名称）**字段中输入 LDAP 服务器的 IP 地址或主机名称。
2. 在 **Port（端口）**字段中输入端口号（默认值为 389）。
3. 如果要启用安全 LDAP（一个非标准协议，也称为 LDAP over SSL），请勾选 **Enable secure LDAP（启用安全 LDAP）**复选框。

   请注意，勾选此复选框会将默认端口号改为 636。
4. 在 **Username（用户名）**和 **Password（密码）**字段中输入此设备的用户名和密码。Username（用户名）字段可包含用户的用户名、电子邮件地址或识别名称。
5. 在 **Search domain（搜索域）**字段中输入 LDAP 服务器的搜索域名。此值在应用搜索过滤器时使用。
6. **Search filter（搜索过滤器）**字段应包含标准 LDAP 查询，可以使用验证变量，例如 %user%、%domain% 和 %email%。
7. 选择 **Mirror（镜像）**或 **Cache address（缓存地址）**作为缓存设置。
   - **Mirror（镜像）**设置可通过同步缓存与 LDAP 服务器中存储的所有地址，一次性全部缓存有效的地址。在以后的任何时间，都可以手动同步缓存与 LDAP 服务器，方法是在 User Directories（用户目录）页面中对此目录单击 **Synchronize（同步）**操作。
   - **Cache address（缓存地址）**设置可使缓存动态更新。新的有效地址在通过 LDAP 服务器验证之后就会缓存。单击 **Clear cache（清除缓存）**可从缓存中删除所有地址。
8. 在 Cache Timeout（缓存超时）字段中输入值。超时是指有效地址在内存缓存中保留的时长。如果在此超时期间，之前验证过的地址发送了电子邮件，该电子邮件会直接传递，而不连接验证服务器。不过，如果此地址在超时之后发送另一封邮件，将会连接服务器以验证地址。默认值为 60 分钟。

IBM LDAP Server Directory

IBM LDAP Server Directory 在 IBM 服务器上提供用户信息管理。请按照下列步骤在 User Directory Properties（用户目录属性）部分配置 IBM LDAP Server Directory:

1. 在 **Server IP address or host name（服务器 IP 地址或主机名称）**字段中输入 LDAP 服务器的 IP 地址或主机名称。
2. 在 **Port（端口）**字段中输入端口号（默认值为 389）。
3. 如果要启用安全 LDAP（一个非标准协议，也称为 LDAP over SSL），请勾选 **Enable secure LDAP（启用安全 LDAP）**复选框。

   请注意，勾选此复选框会将默认端口号改为 636。
4. 在 **Username（用户名）**和 **Password（密码）**字段中输入此设备的用户名和密码。Username（用户名）字段可包含用户的用户名或识别名称。
5. 选择 **Mirror（镜像）**或 **Cache address（缓存地址）**作为缓存设置。
   - **Mirror（镜像）**设置可通过同步缓存与 LDAP 服务器中存储的所有地址，一次性全部缓存有效的地址。在以后的任何时间，都可以手动同步缓存与 LDAP 服务器，方法是在 User Directories（用户目录）页面中对此目录单击 **Synchronize（同步）**操作。
   - **Cache address（缓存地址）**设置可使缓存动态更新。新的有效地址在通过 LDAP 服务器验证之后就会缓存。单击 **Clear cache（清除缓存）**可从缓存中删除所有地址。
6. 在 Cache Timeout（缓存超时）字段中输入值。超时是指有效地址在内存缓存中保留的时长。如果在此超时期间，之前验证过的地址发送了电子邮件，该电子邮件会直接传递，而不连接验证服务器。不过，如果此地址在超时之后发送另一封邮件，将会连接服务器以验证地址。默认值为 60 分钟。

通用 LDAP Server Directory

通用 LDAP 目录提供任何 LDAP 服务器都支持的用户信息管理。请按照下列步骤在 User Directory Properties（用户目录属性）部分配置通用 LDAP Server Directory:

1. 在 **Server IP address or host name（服务器 IP 地址或主机名称）**字段中输入 LDAP 服务器的 IP 地址或主机名称。
2. 在 **Port（端口）**字段中输入端口号（默认值为 389）。
3. 如果要启用安全 LDAP（一个非标准协议，也称为 LDAP over SSL），请勾选 **Enable secure LDAP（启用安全 LDAP）**复选框。

   请注意，勾选此复选框会将默认端口号改为 636。
4. 在 **Username（用户名）**和 **Password（密码）**字段中输入此设备的用户名和密码。Username（用户名）字段可包含用户的用户名或识别名称。
5. 在 **Search domain（搜索域）**字段中输入 LDAP 服务器的搜索域名。此值在应用搜索过滤器时使用。

6. **Search filter（搜索过滤器）**字段应包含标准 LDAP 查询，可以使用验证变量，例如 %user%、%domain% 和 %email%。
7. 在 **Mail field（邮件字段）**文本框中输入要导入的可选电子邮件地址。
8. 选择 **Mirror（镜像）**或 **Cache address（缓存地址）**作为缓存设置。
   - **Mirror（镜像）**设置可通过同步缓存与 LDAP 服务器中存储的所有地址，一次性全部缓存有效的地址。在以后的任何时间，都可以手动同步缓存与 LDAP 服务器，方法是在 User Directories（用户目录）页面中对此目录单击 **Synchronize（同步）**操作。
   - **Cache address（缓存地址）**设置可使缓存动态更新。新的有效地址在通过 LDAP 服务器验证之后就会缓存。单击 **Clear cache（清除缓存）**可从缓存中删除所有地址。
9. 在 Cache Timeout（缓存超时）字段中输入值。超时是指有效地址在内存缓存中保留的时长。如果在此超时期间，之前验证过的地址发送了电子邮件，该电子邮件会直接传递，而不连接验证服务器。不过，如果此地址在超时之后发送另一封邮件，将会连接服务器以验证地址。默认值为 60 分钟。

收件人列表

收件人列表是包含电子邮件地址列表及其关联密码（每行一组）的文本文件。此文件可用于用户收件人验证。

可以使用 Recipient List（收件人列表）表格顶部的关键字输入字段和 Search（搜索）按钮对收件人执行关键字搜索。搜索结果出现后，可使用 **View All（查看所有）**选项查看整个收件人列表。

请按照下列步骤在 User Directory Properties（用户目录属性）部分配置收件人列表:

1. 通过单击 **Recipient information file（收件人信息文件）**输入字段旁边的 **Browse（浏览）**并导航到所需的文本文件，添加预定义的收件人列表文件。文件格式应为每行 1 个电子邮件地址及密码，最多可容纳 1000 个条目。

   注
   如果在已经有活动的收件人列表的情况下添加新收件人列表文件，新文件将覆盖当前文件。

2. 也可以通过下列方法创建收件人列表：在 **Enter Recipient Information（输入收件人信息）**框中输入个别电子邮件地址及关联的密码，然后单击箭头按钮添加信息到右侧的 **Recipient List（收件人列表）**框中。
3. 如果要对收件人列表执行关键字搜索，请单击 **Search（搜索）**。
4. 单击 **OK（确定）**。

在完成收件人列表条目之后，可以单击 **Export（导出）**将列表作为文本文件导出至本地驱动器。

在 **Recipient List（收件人列表）**框中选择个别条目并单击 **Delete（删除）**可将其删除。

ESMTP Server Directory

ESMTP Server Directory 使用扩展 SMTP 中的功能提供用户身份验证和收件人验证。请按照下列步骤在 User Directory Properties（用户目录属性）部分配置 ESMTP Server Directory:

1. 确定需要的电子邮件验证方法。选择 **Use the return status of the VRFY command（使用 VRFY 命令的返回状态）**验证电子邮件用户名。选择 **Use the return status of the RCPT command（使用 RCPT 命令的返回状态）**验证电子邮件收件人。
2. 在 **Sender email address（发件人电子邮件地址）**字段中输入用户目录的电子邮件地址。
3. 在 Cache Timeout（缓存超时）字段中输入值。缓存超时是指有效地址在内存缓存中保留的时长。如果在此超时期间，之前验证过的地址发送了电子邮件，该电子邮件会直接传递，而不连接验证服务器。不过，如果此地址在超时之后发送另一封邮件，将会连接服务器以验证地址。默认值为 60 分钟。

   单击 **Clear cache（清除缓存）**可从缓存中删除所有地址。

管理域和 IP 地址组

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

可在一个组中定义域名或 IP 地址的集合以用于 Email Security Gateway 功能。例如，您可以定义域名组来建立基于域的传送选项，也可以定义不对其执行信誉服务、实时黑名单 (RBL) 或目录攻击防护扫描的 IP 地址组。IP 地址组也可用于电子邮件加密功能。

可以在域组或 IP 地址组上执行以下操作:

- *添加域组*
- *编辑域组*
- *添加 IP 地址组*
- *编辑 IP 地址组*

应注意以下两个特殊的默认域组或 IP 地址组:

- 受保护域组
- 受信任的 IP 地址组

有关使用加密网关默认 IP 地址组的信息，请参阅*第三方加密应用程序*（第 109 页）。无法删除默认组。

受保护域组

Protected Domain（受保护的域）组应包含组织拥有的、需要 Email Security Gateway 保护的所有域。Email Security 中的邮件方向根据组织受保护域确定:

- 入站 — 发件人地址不来自受保护域，收件人地址处于受保护域中
- 出站 — 发件人地址来自受保护域，收件人地址不处于受保护域中
- 内部 — 发件人和收件人地址均处于受保护域中。

如果发件人和收件人地址均不在受保护域，则会执行开放转发。

除非已在首次配置向导的 Domain-based Route（基于域的路由）页面中输入了受保护的域名，否则在安装 Email Security 之后，默认的 Protected Domain（受保护的域）组为空。域可能添加到 Protected Domain（受保护的域）组或从中删除，但无法删除 Protected Domain（受保护的域）组自身。

重要事项

确保 Protected Domain（受保护的域）组包含 Email Security 将要保护的所有域。

如果邮件从未受保护的域发送至组织中未受保护的域，将会产生开放转发。因此，Email Security 可能会拒绝来自未受保护的任何域的所有邮件。从外部受信任的 IP 地址发送到组织中未受保护域的邮件将绕过分析并进行传送。

混合服务在混合服务注册期间使用 Protected Domain（受保护的域）组验证在其传送路由中指定的域是否全部来自此组。如果需要通过多个 SMTP 服务器定义基于域的传送路由，则不应将 Protected Domain（受保护的域）组用于配置 Email Security Gateway 传送路由（在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Mail Routing（邮件路由）**页面中）。有关信息，请参阅基于域的路由（第 85 页）。

受信任的 IP 地址组

与 Protected Domain（受保护的域）组一样，Trusted IP Addresses（受信任的 IP 地址）默认组在安装 Email Security 之后为空。IP 地址可添加到 Trusted IP Addresses（受信任的 IP 地址）组或从中删除，但无法删除 Trusted IP Addresses（受信任的 IP 地址）组自身。Trusted IP Addresses（受信任的 IP 地址）组最多可包括 1024 个地址。

受信任的 IP 地址可能包括内部邮件服务器或受信任的合作伙伴邮件服务器。

来自 Trusted IP Addresses（受信任的 IP 地址）组中地址的邮件可能会绕过某些入站电子邮件过滤。使用 Trusted IP Addresses（受信任的 IP 地址）组可能会增加电子邮件处理时间。

具体而言，来自受信任的 IP 地址的邮件可以绕过以下电子邮件过滤:

- 全局 Always Block（始终拦截）列表（**Main（主页）> Policy Management（策略管理）> Always Block/Permit（始终拦截 / 始终允许）**）
- 邮件大小限制以外的所有邮件控制（**Settings（设置）> Inbound/Outbound（入站 / 出站）> Message Control（邮件控制）**）
- 收件人验证（**Settings（设置）> Users（用户）> User Authentication（用户身份验证）**）
- 所有连接控制（**Settings（设置）> Inbound/Outbound（入站 / 出站）> Connection Control（连接控制）**）
- 目录搜集攻击（**Settings（设置）> Inbound/Outbound（入站 / 出站）> Directory Attacks（目录攻击）**）
- 转发控制（**Settings（设置）> Inbound/Outbound（入站 / 出站）> Relay Control（转发控制）**）

> **注**
> 来自受信任的 IP 地址的邮件不绕过策略和规则应用程序，并且始终进行防垃圾邮件和防病毒过滤。

您可以选中名称右边的复选框并单击 **Delete（删除）**，从相应的列表中删除域或 IP 地址组。

添加域组

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 **Settings（设置）> Users（用户）> Domain Groups（域组）**页面上单击 **Add（添加）**打开 Add Domain Group（添加域组）页面。按照下列步骤添加域组:

1. 在 **Domain Group Name（域组名称）**字段中输入新域组的名称。
2. 输入域组的简短说明。

在 Domain Group Details（域组详细信息）部分，单击 **Domain address file（域地址文件）**字段旁边的 **Browse（浏览）**并导航至所需的文本文件以添加预定义的域组。文件格式应为每行 1 个域地址，并且文件最大不得超过 10 MB。如果文件包含任何无效的条目，Email Security 只接受有效的条目，而拒绝无效的条目。

1. 还可以通过下列方式创建域组：在 **Domain Address（域地址）**字段中输入个别域地址，然后单击箭头按钮将信息添加到右侧的 **Added Domains（已添加的域）**框中。使用通配符包含子域条目（例如 *.domain.com）。
2. 单击 **OK（确定）**。

在完成域地址条目的添加之后，可以单击已添加域的 **Export（导出）**按钮将列表作为文本文件导出至本地驱动器。

在 **Added Domains（已添加的域）**框中选择个别条目并单击 **Delete（删除）**可将其删除。

编辑域组

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

要编辑域组，请在 **Settings（设置）> Users（用户）> Domain Groups（域组）** Domain Groups List（域组列表）中单击域组名称以打开 Edit Domain Group（编辑域组）页面。在此页面添加或删除个别域。也可以编辑域组说明。

请注意，如果某个域正在使用中，您需要确认涉及该域的任何更改。

添加 IP 地址组

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> IP Groups（IP 组）** 页面上单击 **Add（添加）**打开 Add IP Address Group（添加 IP 地址组）页面。按照下列步骤添加 IP 地址组:

1. 在 **IP Address Group Name（IP 地址组名称）**字段中输入新 IP 地址组的名称。
2. 输入 IP 地址组的简短说明。
3. 通过单击 **IP address file（IP 地址文件）**字段旁边的 **Browse（浏览）**并导航到所需的文本文件，添加预定义的 IP 地址组。文件格式应为每行 1 个 IP 地址，并且文件最大不得超过 10 MB。

   注

   默认的加密网关 IP 地址组仅支持单一的 IP 地址条目。子网地址条目被视为无效，并且不被该 IP 地址组接受。

   可为其他默认和自定义 IP 地址组输入子网地址。

4. 还可以通过另一种方法创建 IP 地址组：在 **IP Address（IP 地址）**框中输入个别 IP 地址，然后单击箭头按钮将信息添加到右侧的 **Added IP Addresses（已添加 IP 地址）**框。
5. 单击 **OK（确定）**。

在完成 IP 地址条目的添加之后，可以单击 Added IP Addresses（已添加的 IP 地址）的 **Export（导出）**按钮将列表作为文本文件导出至本地驱动器。

在 **Added IP Addresses（已添加的 IP 地址）**框中选择个别条目并单击 **Remove（删除）**可将其删除。

编辑 IP 地址组

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

要编辑 IP 地址组，可在 IP Address Groups List（IP 地址组列表）中单击该 IP 地址组名称以打开 Edit IP Address Group（编辑 IP 地址组）页面。在此页面添加或删除个别 IP 地址。也可以编辑 IP 地址组说明。

请注意，如果某个 IP 地址正在使用中，您需要确认涉及该地址的任何更改。

管理用户验证 / 身份验证选项

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在定义域组之后，可以为创建的用户目录中的用户确定收件人验证及用户身份验证设置。有关创建域组的信息，请参阅管理域和 *IP* 地址组（第 58 页）。

Email Security Gateway 中提供三类用户验证 / 身份验证:

- **收件人验证** — 在接收邮件之前验证邮件收件人
- **SMTP 身份验证** — 在接收邮件之前对邮件发件人进行身份验证
- **Personal Email 身份验证** — 在访问 Personal Email Manager 工具以管理被阻止的电子邮件之前对用户进行身份验证。有关 Personal Email Manager 最终用户工具的详细信息，请参阅配置 *Personal Email Manager* 最终用户选项（第 157 页）。
- **分发列表验证** — 验证电子邮件分发列表的各个成员

域组中的用户将根据相应的用户目录予以验证，并且应用指定的身份验证设置。如果您希望使用分发列表验证选项，确保在用户目录中包括组电子邮件地址。

重要事项

可以创建多个 Personal Email Manager 用户身份验证组。但任何受保护的域组（在 **Settings（设置）> Users（用户）> Domain Groups（域组）**）只能包含在一个 Personal Email Manager 用户身份验证组中。

将受保护的域组包含在多个 Personal Email Manager 用户身份验证组中，可能会导致该域组的用户无法访问 Personal Email Manager 工具。

请确保将包含该受保护域组中用户的所有用户目录添加到关联的 Personal Email Manager 身份验证组。

单击 **Add（添加）**创建新的收件人验证 / 身份验证设置。

单击现有身份验证设置的名称可修改设置。

要删除一组身份验证设置，请在 User Authentication（用户身份验证）页面中选择该组设置，勾选设置名称旁边的复选框，单击 **Delete（删除）**。

添加用户身份验证设置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用 **Settings（设置）> Users（用户）> User Authentication（用户身份验证）**页面可为域 / 用户目录组添加新的用户验证 / 身份验证设置。

1. 单击 **Add（添加）**以打开 Add User Authentication（添加用户身份验证）页面。
2. 为这组身份验证设置指定名称。
3. 选择要应用的用户验证 / 身份验证设置的类型：收件人验证、SMTP 身份验证、Personal Email 身份验证或分发列表验证。

   如果指定 SMTP 身份验证，必须确保为出站和内部转发选择 **Allow relays only for senders from trusted IP addresses（仅对受信任 IP 地址中的发件人允许转发）**选项（**Settings（设置）> Inbound/Outbound（入站 / 出站）> Relay Control（转发控制）**）。
4. 选择要作为身份验证设置目标的域组。

   要在域组中添加或删除域名，可以在 User Authentication（用户身份验证）页面的 Domains（域）区域中单击 **Edit（编辑）**以打开 Edit Domain Group（编辑域组）页面。您在此所做的更改也会反映在 **Settings（设置）> Users（用户）> Domain Groups（域组）**页面中。
5. 勾选目录名称旁边的复选框，然后单击箭头按钮将其添加到 Recipients（收件人）框中，以选择要应用这些身份验证设置的相应用户目录。

   如果要为这些身份验证设置创建新的用户目录，请单击 **Add user directory（添加用户目录）**。Add User Directory（添加用户目录）页面将会打开，让您创建新的目录。有关用户目录创建说明，请参阅添加和配置用户目录（第 54 页）。

   您可以选择用户目录参考并单击 **Delete（删除）**，将其从 Recipients（收件人）框中删除。此操作将从 Recipients（收件人）列表中移除该用户目录，但不会将其从 **Settings（设置）> Users（用户）> User Directories（用户目录）**页面中删除。

编辑用户身份验证设置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 User Authentication（用户身份验证）页面中单击设置名称，以编辑现有的身份验证设置。在 Edit User Authentication（编辑用户身份验证）页面中更改任何设置。有关身份验证设置的信息，请参阅添加用户身份验证设置（第 63 页）。

请注意，可以在用户验证 / 身份验证设置中添加或删除用户目录。用户目录条目在 **Settings（设置）> Users（用户）> User Directories（用户目录）**页面中修改。

管理传输层安全性 (TLS) 证书

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

传输层安全性 (TLS) 是一个为电子邮件通信提供额外安全保护层的协议。使用此协议有助于防止不受信任的路由器等设备允许第三方监视或改变服务器与客户端之间的通信。Email Security 可接收通过 TLS 传输的邮件，也可通过此协议发送邮件到特定的域。

对于入站连接，默认的 TLS 证书随 Email Security Gateway 提供。安装 Email Security 之后，默认的 TLS 证书信息显示在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> TLS Certificate（TLS 证书）**页面的 TLS Certificate for Incoming Connection（入站连接 TLS 证书）部分。详细信息包括证书版本、序列号、颁发机构和到期日期。

在默认证书到期时可以生成新的证书。在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> TLS Certificate（TLS 证书）**页面中，单击 **Generate（生成）**创建新的证书。请注意，生成新的证书会覆盖目前存在的任何证书。

提供 TLS 证书的导入和导出功能。

也可以为出站连接管理受信任的证书颁发机构 (CA) 颁发的证书。TLS Certificate（TLS 证书）页面上的表格显示了证书的相关信息，包括常见名称、颁发机构，以及到期日期。您可以使用导入功能，浏览至受信任证书所在的位置，并将其添加到 Trusted CA Certificate for Outgoing Connection（出站连接受信任的 CA 证书）表格中。也可以使用搜索功能，对所有受信任的 CA 证书执行关键字搜索。

有关导入和导出 TLS 和 CA 证书的详细信息，请参阅以下各节:

- 导入 *TLS* 证书（第 65 页）
- 导出 *TLS* 证书（第 65 页）
- 导入受信任的 *CA* 证书（第 65 页）

导入 TLS 证书

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可能希望导入证书，而不是在 Email Security Gateway 中生成新证书。请注意，导入证书会覆盖目前存在的任何证书。

按照以下步骤导入网络上已有的证书:

1. 在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> TLS Certificate（TLS 证书）**页面中，单击 **Import（导入）**。
2. 在确认对话框中单击 **Yes（是）**。Import Certificate（导入证书）区域将显示在 Import（导入）按钮下。
3. 使用 **Browse（浏览）**可导航至证书文件。选择文件时，其文件名将出现在 **Certificate file（证书文件）**字段中。文件格式必须为 .p12 或 .pfx。
4. 在 **Password（证书密码）**字段中输入密码（最大长度为 100 个字符）。
5. 单击 **OK（确定）**。

导出 TLS 证书

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

如果要将 TLS 证书和密码导出到网络上的某个位置，请单击 **Export（导出）**。在 Save（保存）框中，浏览至要存储证书及密码的位置。

导入受信任的 CA 证书

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

按如下方式导入受信任的 CA 证书:

1. 在 Trusted CA Certificate for Outgoing Connection（出站连接受信任的 CA 证书）部分，单击 **Import（导入）**。
2. 在 Import Trusted CA Certificate（导入受信任的 CA 证书）对话框中，输入所需证书的文件名，或浏览至网络中的所在位置。
3. 单击 **OK（确定）**。

证书被添加到受信任的 CA 证书表格中。选择 CA 证书并单击 **Delete（删除）**可从表中移除 CA 证书。

备份和恢复管理器设置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security 管理器维护多个重要的配置设置文件，其中包括

- 数据库配置
- Email Security Gateway 设备列表
- Email Security Gateway 管理员设置
- 演示报表模板和数据

可能需要保留这些设置的备份副本，以便在必须执行系统恢复操作时使用。

备份和恢复实用程序随 Email Security 管理功能安装在管理器上。

备份 / 恢复功能包括备份和恢复日志，其中显示带有时间- 戳的管理器备份和恢复活动。

注
由于备份 / 恢复实用程序会停止 Email Security 管理器服务，因此备份和恢复活动只记录在备份和恢复日志中。

备份设置

Email Security 备份和恢复功能可从 **Settings（设置）> General（一般）> Backup/ Restore（备份 / 恢复）**页面访问。在一台设备上进行的备份和恢复设置会应用于您网络中的所有设备。

要备份 Email Security 管理器配置设置，单击 **Backup（备份）**激活该实用程序，并且指定备份文件的本地文件夹。该文件夹位置出现在页面 Restore Settings（恢复设置）部分的 File Location（文件位置）字段中。

如果要将备份设置保存在 Log Database 服务器上，请在 Backup Settings（备份设置）部分勾选该选项旁边的复选框。在您进行此选择时，Remote Log Database Server Access（远程 Log Database 服务器访问）框将会启用，让您输入以下服务器信息:

- **域名 / 主机名**。如果使用域帐户，请输入域名，否则，输入 SQL Server 机器的主机名。
- **用户名**。输入拥有 SQL Server 登录权限的用户名。
- **密码**。密码不能包含 1 个以上的双引号。

- **备份/恢复文件路径**。输入远程 SQL Server 机器上的共享文件夹路径（例如 \\10.1.1.2\shared\）。

> **注**
> 备份设置的 Email Security 版本必须与当前所安装产品的版本匹配。
>
> 备份设置文件大小不得超过 10 MB。

单击 **Check Status（检查状态）**以确保可访问远程日志数据库服务器。

恢复设置

单击 **Restore（恢复）**可使用 Email Security 备份 / 恢复实用程序将设置恢复到其在 Log Database 服务器上的原始备份状态。恢复功能会检索备份设置的位置，并将它们应用到管理器配置文件。恢复配置设置后，Email Security 将自动重新启动。

配置系统警报

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

除了在仪表盘 Health Alert Summary（健康警报摘要）中显示系统警报之外，Email Security Gateway 还可以使用其他方法向管理员通知发生的各种系统事件。例如，可以发送通知提示更新数据库下载类别和订购问题以及加密和用户目录问题。

使用 **Settings（设置）> Alerts（警报）> Enable Alerts（启用警报）**页面启用和配置所需的通知方式。然后使用 **Settings（设置）> Alerts（警报）> Alert Events（警报事件）**页面启用要为其发送通知的警报类型。

启用系统警报

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

可以使用下列一种或多种传送方法确定警报的分发方式:

- 通过电子邮件发送到指定的个人
- 在 **Main（主页）> Status（状态）> Alerts（警报）**页面上以弹出消息的方式发送到指定的计算机
- 通过 SNMP Trap 系统发送到指定的社区

使用 **Settings（设置）> Alerts（警报）> Enable Alerts（启用警报）**页面可配置警报传递方式。

完成警报方式的启用后，单击 **OK（确定）**。

电子邮件警报

勾选 **Enable email alerts（启用电子邮件警报）**复选框，以电子邮件方式发送警报和通知给管理员。然后配置以下电子邮件设置:

字段	说明
From email address（发件人电子邮件地址）	要用作电子邮件警报发件人的电子邮件地址
Administrator email address (To)（管理员电子邮件地址（收件人））	电子邮件警报主要收件人的电子邮件地址。各个地址之间必须用分号分隔。
Email addresses for completed report notification（接收已完成报表通知的电子邮件地址）	已完成报表通知的收件人电子邮件地址。各个地址之间必须用分号分隔。

弹出警报

勾选 **Enable pop-up alerts（启用弹出警报）**复选框，以通过在特定计算机的 **Main（主页）> Status（状态）> Alerts（警报）**页面上弹出消息的方式来传送警报。然后，输入所需计算机的 IP 地址或机器名称，各个条目之间使用分号分隔。

SNMP 警报

勾选 **Enable SNMP alerts（启用 SNMP 警报）**复选框，以通过网络中安装的 SNMP Trap 系统传送警报消息。提供有关 SNMP Trap 系统的下列信息:

字段	说明
Community name（社区名称）	SNMP Trap 服务器上陷阱社区的名称
Server IP or name（服务器 IP 或名称）	SNMP Trap 服务器的 IP 地址或名称
Port（端口）	SNMP 消息使用的端口号

单击 **Check Status（检查状态）**以向 SNMP 服务器发送测试邮件，并验证指定的 SNMP 端口是否已打开。

警报事件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

为确保管理员收到系统事件（例如数据库下载失败或者订购即将到期）的通知，请配置要通过电子邮件、弹出消息或 SNMP Trap-系统分发的系统警报。

使用 **Settings（设置）> Alerts（警报）> Enable Alerts（启用警报）**页面选择用于将这些警报发送给 Websense 管理员的方法。

使用 **Settings（设置）> Alerts（警报）> Alert Events（警报事件）**页面选择每种警报传递方式要传递的警报类型。警报适用于以下事件类型:

- 订购到期
- Email Security 系统事件
- Log Server 和 Log Database 事件
- 邮件队列事件
- 电子邮件过滤事件
- 加密和解密事件
- 设备集群配置事件
- 用户目录服务器事件
- 混合服务操作事件
- 特征码更新事件
- SIEM 服务器事件
- Personal Email Manager 服务器事件
- 入站未传送的电子邮件事件

为 Alerts（警报）列表中的每种事件类型勾选要使用的传递方式。勾选每种警报传递方式的列标题可选择该列中的所有事件类型。必须在 Enable Alerts（启用警报）页面中启用某个传送方法，才可为事件类型选择该方法。

可以为入站未传送的电子邮件事件警报类型设置频率阈值。该设置将会在邮件服务器上发生指定数目的入站连接错误后触发警报通知。不会针对此警报监控出站流量。

使用以下步骤设置用于发送入站未传送的电子邮件警报的阈值:

1. 单击 **Configure alert thresholds（配置警报阈值）**链接以打开配置对话框。
2. 输入要触发警报通知的连接错误数。将会在超过该连接阈值后以 30 分钟为间隔发送通知。
3. 单击 **OK（确定）**。

完成所有警报类型和通知的启用后，单击 **OK（确定）**。

4 管理邮件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

主题:

配置邮件属性

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security 邮件控制属性可用于设置邮件大小和数量限制，以及确定如何处理无效收件人。选择 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Message Control（邮件控制）**来配置以下设置:

- 设置大小属性（第 72 页）
- 设置数量属性（第 72 页）
- 配置无效收件人设置（第 73 页）
- 启用存档邮件选项（第 73 页）
- 启用邮件发件人验证（第 73 页）
- 启用退信地址标记验证 *(BATV)*（第 73 页）
- 启用域名密钥识别邮件 *(DKIM)* 验证（第 74 页）

完成设置邮件属性后单击 **OK（确定）**。

设置大小属性

使用 Message Size Options（邮件大小选项）配置邮件大小属性:

1. 如果要设置最大邮件大小，请选择 **Limit message size（限制邮件大小）**（默认设置）。
2. 在相应的 **Maximum message size（最大邮件大小）(KB)** 字段输入最大邮件大小，输入值范围 1 - 102400（默认值为 10240）。此设置可防止非常大的邮件占用宝贵的带宽。
3. 如果要设置每个连接的最大邮件大小，请选择 **Limit data size per connection（限制每个连接的数据大小）**。
4. 在相应的 **Maximum data size（最大数据大小）(KB)** 字段输入最大数据大小，输入值范围 1 - 204800（默认值为 20480）。此设置有助于限制接收附带极大附件的邮件，从而避免其占用宝贵的带宽。

设置数量属性

使用 Message Volume Options（邮件数量选项）配置邮件数量属性:

1. 选择 **Limit number of messages per connection（限制每个连接的邮件数量）**以启用该选项。
2. 在相关的 **Maximum number of messages（邮件最大数量）**字段输入每个连接的最大邮件数量，输入值范围 1 - 65535（默认值为 30）。

3. 选择 **Limit number of recipients per message（限制每封邮件的收件人数量）**以启用该选项。
4. 在相应的 **Maximum number of recipients（收件人最大数量）**字段输入收件人的最大数量，输入值范围 1 - 4096（默认值为 20）。这有助于防止一封邮件发送给数百个用户，从而节省带宽。

配置无效收件人设置

使用 Invalid Recipient Options（无效收件人选项）配置无效收件人设置:

1. 如果要允许包含无效收件人的邮件进入您的系统，请勾选 **Allow invalid recipients（允许无效收件人）**复选框。此选项仅当使用收件人验证时才可用（请参阅 **Settings（设置）> Users（用户）> User Authentication（用户身份验证）**）。
2. 输入无效收件人百分比的值以确定是否阻止邮件（默认值为 100）。
3. 勾选适当的复选框以允许系统在邮件未被阻止时发送未送达回执 (NDR) 通知。

启用存档邮件选项

如果要在扫描所有入站邮件之前将其保存到存档邮件队列，请勾选 **Enable archive queue storage（启用存档队列存储）**复选框。请注意，启用此功能可能会影响存储容量和系统性能。默认情况下禁用此选项。

在 **Main（主页）> Message Management（邮件管理）> Message Queues（邮件队列）**页面上单击队列列表中的 **archive（存档）**，可查看存档队列。

启用邮件发件人验证

通过启用内部发件人验证功能，确保内部电子邮件发件人是经过身份验证的用户。此操作执行检查，以确认来自内部域的电子邮件发件人也是经过身份验证的用户。要使电子邮件通过此检查功能，邮件发件人地址必须符合身份验证条目中的发件人记录。

在 Internal Sender Verification（内部发件人验证）部分勾选 **Enable internal sender verification（启用内部发件人验证）**复选框以激活此功能。默认情况下，此功能被禁用。

启用退信地址标记验证 (BATV)

退信地址标记验证 (BATV) 是一种确定受保护域中的退信地址是否有效的方法。此方法有助于防止反向散射的垃圾邮件 - 退回组织的邮件中包含伪造的收件人地址。

启用 BATV 后，Email Security Gateway 使用独特的标签标记出站邮件的发件人地址。退回该收件人的邮件经过检查，确认其是否含有该独特标签。如果 Email Security 检测到标签，则传送退回的邮件。不含标签的退回邮件被阻止。

在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Message Control（邮件控制）**页面中启用 BATV。在 Bounce Address Tag Validation（退信地址标记验证）部分勾选 **Enable Bounce Address Tag Validation（启用退信地址标记验证）**复选框。

您可能希望来自某些用户和 IP 地址组的邮件能够绕过 BATV 功能。这些组可在 Bounce Address Tag Validation（退信地址标记验证）部分中定义。从以下下拉列表中选择组:

- 入站 IP 地址组
- 入站域组
- 出站域组

请注意，选为出站绕过的域组也必须选为入站绕过。

每个组的默认设置为 **None（无）**。只有用户定义的域和 IP 地址组在下拉列表中可用。有关创建域和 IP 地址组的信息，请参阅管理域和 *IP* 地址组（第 58 页）。

启用域名密钥识别邮件 (DKIM) 验证

域名密钥识别邮件 (DKIM) 是一种使用邮件头数字签名将域名与电子邮件进行关联的验证方法。Email Security Gateway 具有 DKIM 签名验证功能，可以从 DNS 检索签名人信息，包括公钥。Email Security 分析并验证签名人信息，以确定邮件的合法性。

可以在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Message Control（邮件控制）**页面的 DomainKeys Identified Mail (DKIM) Verification（域名密钥识别邮件 (DKIM) 验证）部分启用 Email Security Gateway DKIM 验证功能。勾选以下任意复选框以激活 DKIM 验证:

- **Enable DomainKeys Identified Mail (DKIM) verification for inbound messages（启用入站邮件域名密钥识别邮件 (DKIM) 验证）**
- **Enable DomainKeys Identified Mail (DKIM) verification for outbound messages（启用出站邮件域名密钥识别邮件 (DKIM) 验证）**
- **Enable DomainKeys Identified Mail (DKIM) verification for internal messages（启用内部邮件域名密钥识别邮件 (DKIM) 验证）**

默认情况下不勾选这些复选框。

您可以配置自定义内容策略过滤器以扫描邮件头中的 DKIM 签名，以及在邮件头触发过滤器时采取的过滤器操作。有关创建该过滤器的信息，请参阅自定义内容（第 112 页）。

管理连接选项

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

通过限制 Email Security Gateway 的并发连接数量，可改善系统的性能。在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Connection Control（连接控制）** 页面的 Connection Options（连接选项）部分，输入每个 IP 地址允许的最大并发连接数量，输入值范围 1 - 500（默认值为 10）。指定连接断开之前允许的最大闲置秒数，输入值范围 1 - 43200（默认值为 300）。

在 Connection Control（连接控制）页面中还可以配置以下设置:

- *使用实时黑名单 (RBL)*（第 75 页）
- *使用反向 DNS 验证*（第 76 页）
- *使用 Websense 信誉服务*（第 77 页）
- *延迟 SMTP 问候*（第 77 页）
- *启用 SMTP VRFY 命令*（第 77 页）
- *更改 SMTP 端口*（第 78 页）
- *使用访问列表*（第 78 页）

如果您想收集和查看一些连接的详细信息，可以启用一项 Email Security 功能，将这些详细信息保存在邮件处理日志中，通过 Websense® V-Series™（V 系列）设备访问。当启用该功能时，无论连接控制自身是否已启用，日志都会收集详细数据。该功能可用于以下连接控制选项:

- 实时黑名单 (RBL)
- 反向 DNS 查找
- 信誉服务
- SMTP 问候延迟

完成配置连接控制设置后单击 **OK（确定）**。

使用实时黑名单 (RBL)

实时黑名单 (RBL) 是第三方发布的已知垃圾邮件来源 IP 地址列表。启用 RBL 检查后，将会阻止来自 RBL 中所列发件人的邮件进入您的系统。Email Security Gateway 支持使用 Spamhaus Datafeed 服务器或输入最多 3 个第三方 RBL 进行 RBL 查询。

在 Real-time Blacklist (RBL) Options（实时黑名单 (RBL) 选项）部分，勾选 **Perform RBL check（执行 RBL 检查）**复选框以启用 RBL 检查。选择下列 RBL 查询方法之一:

- **Spamhaus 服务**。使用 Spamhaus 服务器进行 RBL 查询
- **域地址**。输入要使用的 RBL 服务的最多 3 个域地址。使用英文分号 (;) 分隔多个地址。

默认情况下不启用此功能。

勾选 **Save connection details in the mail processing log（将连接详情保存到邮件处理日志中）**复选框，可将详细的连接信息保存到设备邮件处理日志中。如果启用该选项，确保在 **Domain address（域地址）**字段中输入至少 1 个第三方 RBL。

使用反向 DNS 验证

反向 DNS 查找使用指针 (PTR) 记录确定与各个发件人 IP 地址相关的域名。通过反向 DNS 查找，Email Security 确保发送到您的系统的电子邮件来自合法的域。使用该选项可以增强对商业群发电子邮件的检测。有关该类型电子邮件的信息，请参阅商业群发电子邮件（第 118 页）。

但是，请注意，如果启用反向 DNS，服务器的性能可能会受到影响，合法用户也可能会被拒绝。默认情况下不启用此功能。

在 Reverse DNS Lookup Options（反向 DNS 查找选项）部分勾选 **Enable reverse DNS lookup（启用反向 DNS 查找）**复选框，可激活反向 DNS 功能。随后，可以通过选择以下一个或多个选项，确定 Email Security 对反向 DNS 查找的响应:

- **Disconnect if the PTR record does not exist.（如果 PTR 记录不存在，则断开连接。）**
- **Disconnect if the PTR record does not match the A record.（如果 PTR 记录与 A 记录不符，则断开连接。）**
- **Disconnect if a soft failure occurs during a reverse DNS lookup.（如果在反向 DNS 查找过程中发生软故障，则断开连接。）**

  如果选择该选项，Email Security Gateway 将在以下事件发生时终止连接:

  - 指定的 DNS 查询缓存服务关闭。
  - 您的 DNS 服务器关闭。
  - 在 DNS 查询期间发生超时。
- **Disconnect if the PTR record does not match the SMTP EHLO/HELO greeting.（如果 PTR 记录与 SMTP EHLO/HELO 问候不符，则断开连接。）**

勾选 **Save connection details in the mail processing log（将连接详情保存到邮件处理日志中）**复选框，可将详细的连接信息保存到设备邮件处理日志中。

使用 Websense 信誉服务

Email Security Gateway 可根据 Websense 信誉服务检查电子邮件发件人的 IP 地址，该服务根据过去的行为对电子邮件发件人进行分类。通过此功能，Email Security 可阻止来自已知垃圾邮件发件人的邮件。

要使用 Websense 信誉服务，请在 Reputation Service Options（信誉服务选项）部分勾选 **Enable Reputation Service（启用信誉服务）**复选框（默认设置）。然后选择以下扫描级别之一以指定阻止邮件的阈值:

- **Conservative（谨慎）**，100% 的时间阻止发送垃圾邮件的地址发出的邮件。
- **Medium（中等）**，99% 的时间阻止发送垃圾邮件的地址发出的邮件。
- **Aggressive（大胆）**，97% 的时间阻止发送垃圾邮件的地址发出的邮件。
- **Custom（自定义）**，可用于输入自定义垃圾邮件百分比。Email Security Gateway 在指定百分比的时间阻止发送垃圾邮件的地址发出的邮件。

勾选 **Save connection details in the mail processing log（将连接详情保存到邮件处理日志中）**复选框，可将详细的连接信息保存到设备邮件处理日志中。

延迟 SMTP 问候

您可以指定 SMTP 问候延迟特定的时间间隔，如果客户端试图在此时间间隔期内发送数据，则其连接会断开。此选项有助于防止垃圾邮件应用程序快速发送高数量的邮件。只要在 SMTP 服务器准备就绪之前向其发送电子邮件，连接就会断开。

通过在 SMTP Greeting Delay Options（SMTP 问候延迟选项）部分勾选 **Enable SMTP greeting delay（启用 SMTP 问候延迟）**复选框，启用 SMTP 问候延迟。指定延迟时间（以秒为单位），输入值范围 1 - 60（默认值为 3）。

默认情况下不启用此功能。

勾选 **Save connection details in the mail processing log（将连接详情保存到邮件处理日志中）**复选框，可将详细的连接信息保存到设备邮件处理日志中。

启用 SMTP VRFY 命令

SMTP VRFY 命令可用于验证电子邮件用户名。在收到验证用户名的请求时，收件服务器将响应用户的登录名。在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Connection Control（连接控制）**页面的 SMTP VRFY Command Option（SMTP VRFY 命令选项）部分勾选 **Enable SMTP VRFY command（启用 SMTP VRFY 命令）**复选框（默认设置）以启用该命令。

重要事项

请谨慎使用此命令。该命令虽然有助于验证用户，但如果用户信息被人恶意窃取，则会造成网络安全问题。

更改 SMTP 端口

Email Security Gateway 的默认 SMTP 端口号为 25。需为 SMTP 使用端口 25，方可与 Email Security Gateway Anywhere 混合服务正确通信。

不过，如果出于任何原因需要自定义该端口号，可以在 SMTP Port Option（SMTP 端口选项）部分中的 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Connection Control（连接控制）**页面进行更改。有效值介于 25 和 5000 之间。

> **注**
> 更改该端口设定后，Email Security Gateway 服务会重启。

使用访问列表

通过访问列表可以指定不对其执行某些电子邮件扫描的 IP 地址组。通过 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Connection Control（连接控制）**页面中的 Allow Access List Options（允许访问列表选项），可识别这些 IP 地址。来自这些地址的邮件可绕过以下电子邮件过滤器扫描:

- 每个 IP 地址的连接数
- RBL 检查
- 反向 DNS 查找
- 信誉服务
- SMTP 问候延迟
- 目录搜集攻击防护
- 入站转发控制

由于来自 Trusted IP Address group（受信任的 IP 地址组）的邮件可绕过更多电子邮件过滤，因此，该组不应被放入 Allow Access List（允许访问列表）。有关详细信息，请参阅管理域和 *IP* 地址组（第 58 页）。

在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> IP Groups（IP 组）**中定义 IP 地址组。在该页面中定义的组显示在 Connection Control Allow Access List Options（连接控制允许访问列表选项）部分的 **IP Groups（IP 组）**下拉列表中。

要创建和修改访问列表:

1. 在 **IP Group（IP 组）**下拉列表中选择 IP 组名称，从而在 **IP addresses（IP 地址）**列表中显示地址并启用 **Edit（编辑）**按钮。
2. 单击 **Edit（编辑）**，在 Edit IP Groups（编辑 IP 组）页面中修改访问列表。
3. 通过单击 **IP address file（IP 地址文件）**字段旁边的 **Browse（浏览）**并导航到所需的文本文件，添加预定义的 IP 地址组。文件格式应为每行 1 个 IP 地址。

4. 还可以在 **IP Address（IP 地址）**框中输入单个 IP 地址，然后单击箭头按钮将信息添加到右侧的 **Added IP Addresses（已添加 IP 地址）**框。

> **注**
> 在此处对 IP 地址组执行的任何更改都反映在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> IP Groups（IP 组）**页面中。

5. 单击 **OK（确定）**。

完成访问列表后，可将该列表导出到网络中的位置。单击 **Export（导出）**可将访问列表文件保存到其他位置。

通过选择 IP 地址并单击 **Remove（删除）**，可从 Added IP Addresses（已添加的 IP 地址）列表中删除该 IP 地址。

真实源 IP 检测

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

真实源 IP 检测使用邮件头信息和到达 Email Security Gateway 的网络跃点数来确定网络外围第一个发件人的 IP 地址。此功能允许将“连接控制”技术（如实时黑名单和信誉检查）有效应用于发件人信息，即使 Email Security Gateway 位于防火墙或内部邮件中继的下游也可以实现。

可以定义直接中继和网络边缘位置，确定 Email Security Gateway 是否执行真实源 IP 检测。直接中继是指直接与 Email Security Gateway 连接的网络设备。所有来自直接中继设备的邮件都会经过真实源 IP 检测。网络边缘是指直接与 Internet 连接的网络设备（例如防火墙）。

如果您的订购包含电子邮件混合服务，可以将真实源 IP 检测和混合服务分析结合使用。系统会根据成功注册混合服务期间输入的信息，创建一个混合服务 IP 组。该 IP 组会出现在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> True Source IP（真实源 IP）**页面的直接中继 IP 地址列表中。虽然无法直接编辑该 IP 组，但是只要更改混合服务 IP 地址（**Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**），其内容便会随之被修改。

> **注**
> 如果混合服务注册不成功，则 Hybrid Service IP Group（混合服务 IP 组）为空。

勾选 **Use True Source IP Detection with email hybrid service analysis（使用真实源 IP 检测和电子邮件混合服务分析）**复选框，可以启用真实源 IP 检测和混合服务，并在直接中继 IP 地址列表中显示混合服务 IP 组。如果不勾选该复选框，则不会显示混合服务 IP 组。

按照以下步骤在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> True Source IP（真实源 IP）**页面中配置您的 Email Security 直接中继和所有网络边缘设备。

1. 单击 **Add（添加）**，打开 Add Direct Relay IP Address/IP Group（添加直接中继 IP 地址 /IP 组）页面。
2. 输入连接至 Email Security Gateway 的直接中继设备的 IP 地址，或者指定您想要用于直接中继的 IP 组。

   默认情况下，直接中继的跃点数为 1，因为它是最靠近 Email Security Gateway 的网络设备。
3. 在 **Check header（检查邮件头）**输入字段中，输入您想要用于匹配源 IP 检测的邮件头文本。

   如果该字段为空，则会分析邮件的 Received（已收到）字段以检测真实源 IP。
4. 单击 **Add Network Edge（添加网络边缘）**，以添加网络边缘设备的 IP 地址和到 Email Security 的跃点数。

强制 TLS 连接

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以指定到达或来自特定 IP 的连接或域组使用强制性传输层安全性 (TLS) 并确定该连接使用的安全级别。使用 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Enforced TLS Connections（强制性 TLS 连接）**页面，指定 Email Security Gateway 对其强制使用 TLS 连接的 IP 地址或域组。

您可以定义与 Email Security Gateway SMTP 服务器相对应的连接方向。传入连接是指从受保护或外部域或 IP 地址组到 Email Security 的连接。传出连接是指从 Email Security 到受保护或外部域或 IP 地址组的连接。

定义了组后，您可以在传入或传出方向列表中更改其顺序。勾选相应的复选框以选择组，然后使用 **Move Up（上移）**或 **Move Down（下移）**按钮更改列表顺序。

勾选复选框并单击 **Delete（删除）**，可以删除组。

最多可以配置 32 个传入或传出连接。

使用以下步骤添加您想要对其使用 TLS 的传入或传出连接:

1. 单击 **Add（添加）**。
2. 输入强制性 TLS 连接的名称。
3. 在 **Priority order（优先顺序）**下拉列表中选择连接的优先顺序。
4. 指定该连接的安全级别。安全级别选项包括以下几项:
   - **Encrypt（加密）**，最低强制级别，用在所有安全级别中
   - **Encrypt and check CN（加密并检查 CN）**，验证证书的常见名称

- **Verify（检验）**，验证证书来自受信任的 CA
- **Verify and check CN（检验并检查 CN）**，验证证书的常见名称，以及证书来自受信任的 CA

> **重要事项**
> 必须在已导入受信任的 CA 证书的情况下，才能使用 2 个“验证”选项。有关受信任证书的信息，请参阅 *管理传输层安全性 (TLS) 证书*（第 64 页）。

5. 选择以下连接加密强度选项之一:
   - Medium（中级），用到使用 128 位加密的密码套件
   - High（高级），包括密钥长度大于 128 位的大多数密码套件。
6. 定义要对其应用强制性 TLS 连接的 IP 地址或域组。选择以下选项之一:
   - **任何（适用于所有连接）**。该选项适用于任何连接，而无论 IP 或域地址如何。
   - **IP address group（IP 地址组）**。在下拉列表中选择一个现有的 IP 地址组，或使用 **Add New IP Group（添加新 IP 组）**新建一个组。
   - **Domain address group（域地址组）**。在下拉列表中选择一个现有的域地址组，或使用 **Add New Domain Group（添加新域组）**新建一个组。

控制目录搜集攻击

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

目录搜集攻击被可疑来源用于获取对组织内部电子邮件帐户的访问权限。目录攻击不仅会消耗大量的系统资源，还会通过获取电子邮件帐户为电子邮件最终用户带来垃圾邮件问题。通过目录攻击防护设置，可以限制在指定的时间段内来自一个 IP 地址的最大邮件数量和连接数量。

要配置目录攻击控制:

1. 选择 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Directory Attacks（目录攻击）**。
2. 选中 **Limit the number of messages/connections per IP every（限制每个 IP 的邮件 / 连接数量）**复选框以启用目录搜集攻击防护功能。
3. 在下拉列表中设置时间段（从 1 秒至 60 分钟，默认值为 60 秒）。
4. 设置在指定时间段内允许来自单个 IP 地址的最大邮件数量（默认值为 30）。
5. 设置在指定时间段内允许来自单个 IP 地址的最大连接数量（默认值为 30）。
6. 如果启用了目录攻击防护选项，还可以启用相关设置，使系统在发生特定的收件人条件设置时阻止 IP 地址。勾选 **Block the IP address for（阻止 IP 地址）**复选框，然后输入要阻止 IP 地址的时间间隔（默认值为 3 小时）。

7. 输入阻止 IP 地址的条件:
   - 邮件收件人的最大数量（默认值为 5）
   - 收件人中无效地址的最大百分比（默认值为 50%）

   当超过这些收件人限制时，连接会自动断开。

   此选项仅当使用了收件人验证选项时才可用（请参阅添加用户身份验证设置（第 63 页））。

配置转发控制选项

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

通过限制允许服务器转发邮件的域和 IP 地址组，可防止未经授权使用您的邮件系统开放转发。受保护的域在 **Settings（设置）> Users（用户）> Domain Groups（域组）**页面中定义。受信任的 IP 地址组在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> IP Groups（IP 组）**页面中定义。

根据以下步骤在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Relay Control（转发控制）**页面中配置转发控制设置:

1. 在 Inbound Relay Options（入站转发选项）部分，根据发件人域的发件人策略框架 (SPF) 设置任何所需的选项:
   - **Reject mail if no SPF record exists.（如果不存在 SPF 记录，则拒绝邮件。）**
   - **Reject mail if the SPF record does not match the sender's domain and a soft fail occurs.（如果 SPF 记录与发件人域不匹配或出现软故障，则拒绝邮件。）**

     “软故障”结果意味着有关发件人域的检查结果尚无定论。
   - **Reject mail if an SPF error occurs.（如果发生 SPF 错误，则拒绝邮件。）**

   默认情况下不启用这些选项。
2. 在 Bypass SPF Option（绕过 SPF 选项）框中，可以指定要为其绕过 SPF 设置的发件人域组。
   a. 勾选 **Bypass SPF validation for senders in the following domain group（为以下域组中的发件人绕过 SPF 验证）**复选框。
   b. 从 **Domain group（域组）**下拉列表中选择发件人域。
3. 在 Outbound Relay Options（出站转发选项）部分，选择在不需要 SMTP 身份验证时对受保护域中发件人的转发设置。默认设置为 **Allow relays only for senders from trusted IP addresses（仅对受信任 IP 地址中的发件人允许转发）**。

   如果使用 SMTP 身份验证，则必须使用默认设置。

   请注意，允许所有出站转发可能会为您的系统带来安全漏洞。

4. 在 Internal Relay Options（内部转发选项）部分，选择在不需要 SMTP 身份验证时对受保护域之间的邮件的转发设置。默认设置为 **Allow relays only for senders from trusted IP addresses（仅对受信任 IP 地址中的发件人允许转发）**。

   如果使用 SMTP 身份验证，则必须使用默认设置。

   请注意，允许所有出站转发可能会为您的系统带来安全漏洞。

配置传送路由

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Mail Routing（邮件路由）**页面中配置传送路由。可创建以下类型的邮件路由:

- 基于用户目录的路由（第 83 页）
- 基于域的路由（第 85 页）

通过勾选相关复选框并使用 **Move Up（上移）**或 **Move Down（下移）**按钮，可更改基于用户目录或基于域的路由顺序。

复制路由

使用以下步骤在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Mail Routing（邮件路由）**页面中复制路由:

1. 通过勾选路由名称旁边的复选框选择路由。
2. 单击 **Copy（复制）**。新路由显示在路由列表中，其名称为原路由名称后面加上带括号的编号。附加的编号表示原路由副本的创建顺序（1、2、3 等）。
3. 单击新路由名称可根据需要编辑路由属性。

删除路由

如果要删除路由，请勾选路由名称旁边的复选框以选择路由，然后单击 **Delete（删除）**。

请注意，默认的域路由无法删除。

基于用户目录的路由

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

首先扫描基于用户目录条目的传送路由，以匹配电子邮件收件人。然后根据选定的用户目录验证域组条目，以确定是否通过指定的路由传送电子邮件。

添加基于用户目录的路由

使用以下步骤在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Mail Routing（邮件路由）**页面中添加基于用户目录的传送路由:

1. 单击 **Add（添加）**以打开 Add User Directory-based Route（添加基于用户目录的路由）页面。
2. 在 **Name（名称）**字段中输入新路由的名称（长度为 4 - 50 个字符）。
3. 在 **Route order（路由顺序）**下拉列表中选择序号，以确定路由扫描顺序。
4. 在 **Domain group（域组）**下拉列表中从预定义域选择目标域。默认值为 Protected Domain（受保护的域）。域组的相关信息显示在 Domain details（域详细信息）框。

   如果要编辑所选域组，请单击 Edit（编辑）打开 Edit Domain Group（编辑域组）页面。有关详细信息，请参阅编辑域组（第 61 页）。
5. 在 User Directories（用户目录）部分选择要用于定义路由的用户目录。从当前定义的用户目录列表中选择用户目录，然后单击箭头按钮将其移动到 Selected User Directories（所选用户目录）框。

   注
   ESMTP 用户目录不包括在目录列表中。ESMTP 用户目录不能用于基于用户目录的路由。

   如果要添加新的用户目录，请单击 **Add User Directory（添加用户目录）**以打开 Add User Directory（添加用户目录）页面。有关信息，请参阅添加和配置用户目录（第 54 页）。

   如果要从 Recipients（收件人）列表中删除用户目录，请选择它并单击 **Delete（删除）**。
6. 选择传送方法:
   - Based on the recipient's domain (using the Domain Name System [DNS])（基于收件人域（使用域名系统 [DNS]））
   - Based on SMTP server IP address designation (using smart host)（基于 SMTP 服务器 IP 地址指定（使用智能主机））。如果选择此选项，SMTP Server List（SMTP 服务器列表）将打开。
     a. 单击 **Add（添加）**打开 Add SMTP Server（添加 SMTP 服务器）对话框。
     b. 输入 SMTP 服务器 IP 地址或主机名和端口。

c. 勾选 **Enable MX lookup（启用 MX 查找）**复选框以启用 MX 查找功能。

> **重要事项**
>
> 如果在上一个步骤中输入的是 IP 地址，则 MX 查找选项不可用。
>
> 如果在上一个步骤中输入的是主机名，则该选项可用。
>
> - 勾选 **Enable MX lookup（启用 MX 查找）**复选框，用于根据主机名 MX 的记录进行的邮件传送。
> - 如果不勾选该复选框，会根据主机名 A 的记录进行邮件传送。

d. 输入该服务器的优先顺序编号（从 1 到 65535，默认值为 5）。

如果单条路由有多个定义的服务器地址，Email Security 会尝试按服务器的优先顺序来传送邮件。当多条路由的优先顺序相同时，会使用轮询传送机制。

在 SMTP 服务器列表中输入的地址不能超过 16 个。

7. 选择任何所需的安全传送选项。
   a. 如果要电子邮件流量使用随机 TLS 协议，请选择 **Use Transport Layer Security（使用传输层安全性）(TLS)**。
   b. 如果要用户提供凭证，请选择 **Require authentication（需要身份验证）**。在 Authentication Information（身份验证信息）框中输入适当的用户名和密码。需要用户进行身份验证时，必须使用 SMTP 服务器 IP 地址传送方法。

基于域的路由

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

基于域组的传送路由在定义基于用户目录的路由之后进行扫描，以匹配电子邮件收件人。如果基于用户目录的路由确认了匹配，则基于域的路由不需要进行匹配扫描。

> **重要事项**
>
> 如果需要通过多个 SMTP 服务器定义基于域的传送路由，则不应将 **Settings（设置）> Users（用户）> Domain Groups（域组）**页面中定义的受保护的域组用于配置 Email Security Gateway 传送路由。
>
> 创建包含受保护域组子集的域组，以供邮件路由使用。

添加基于域的路由

使用以下步骤在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Mail Routing（邮件路由）**页面中添加基于域的传送路由:

1. 单击 **Add（添加）**以打开 Add Domain-based Route（添加基于域的路由）页面。
2. 在 **Name（名称）**字段中输入新路由的名称。
3. 在 **Route order（路由顺序）**下拉列表中选择序号，以确定路由扫描顺序。
4. 在 **Domain group（域组）**下拉列表中从预定义域选择目标域。默认值为 Protected Domain（受保护的域）。域组的相关信息显示在 Domain details（域详细信息）框。

   如果要编辑所选域组，请单击 Edit（编辑）打开 Edit Domain Group（编辑域组）页面。有关详细信息，请参阅编辑域组（第 61 页）。
5. 选择传送方法:
   - Based on the recipient's domain (using the Domain Name System [DNS])（基于收件人域（使用域名系统 [DNS]））
   - Based on SMTP server IP address designation (using smart host)（基于 SMTP 服务器 IP 地址指定（使用智能主机））。如果选择此选项，SMTP Server List（SMTP 服务器列表）将打开。
     a. 单击 **Add（添加）**打开 Add SMTP Server（添加 SMTP 服务器）对话框。
     b. 输入 SMTP 服务器 IP 地址或主机名和端口。
     c. 勾选 **Enable MX lookup（启用 MX 查找）**复选框以启用 MX 查找功能。

     重要事项

     如果在上一个步骤中输入的是 IP 地址，则 MX 查找选项不可用。

     如果在上一个步骤中输入的是主机名，则该选项可用。

     - 勾选 **Enable MX lookup（启用 MX 查找）**复选框，用于根据主机名 MX 的记录进行的邮件传送。
     - 如果不勾选该复选框，会根据主机名 A 的记录进行邮件传送。

     d. 输入该服务器的优先顺序编号（从 1 到 65535，默认值为 5）。

     如果单条路由有多个定义的服务器地址，Email Security 会尝试按服务器的优先顺序来传送邮件。当多条路由的优先顺序相同时，会使用轮询传送机制。

在 SMTP 服务器列表中输入的地址不能超过 16 个。

6. 选择任何所需的安全传送选项。
   a. 如果要电子邮件流量使用随机 TLS 协议，请选择 **Use Transport Layer Security（使用传输层安全性）(TLS)**。
   b. 如果要用户提供凭证，请选择 **Require authentication（需要身份验证）**。在 Authentication Information（身份验证信息）框中输入适当的用户名和密码。需要用户进行身份验证时，必须使用 SMTP 服务器 IP 地址传送方法。

改写电子邮件和域地址

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

可以改写电子邮件信封收件人地址，将邮件传送重定向至其他地址。也可以改写信封发件人和邮件头地址，从而向邮件收件人掩蔽地址详细信息。在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Address Rewriting（地址改写）**页面中，可以为入站、出站和内部电子邮件配置地址改写。

在显示地址改写列表时，可以单击 **Export（导出）**将列表中的所有电子邮件或域地址导出至文本文件。

选择地址改写列表中的地址之一并单击 **Delete（删除）**，可以从列表中删除电子邮件或域地址。

添加收件人地址改写条目

使用 Inbound Messages（入站邮件）选项卡可以指定入站邮件的收件人地址改写条目，使用 Outbound and Internal Messages（出站和内部邮件）选项卡可以指定出站或内部邮件重定向。电子邮件信封收件人地址将根据 Envelope Recipient Address Rewrite List（信封收件人地址改写列表）中的条目进行改写。

使用下列步骤添加收件人改写条目:

1. 在 Envelope Recipient Address Rewrite List（信封收件人地址改写列表）中单击 **Add（添加）**，打开 Add Recipient Email or Domain Address（添加收件人电子邮件或域地址）页面。
2. 以下列两种方式之一输入地址:
   - 勾选 **Individual email address or domain rewrite entry（单个电子邮件地址或域改写条目）**复选框，并在相应的输入字段中输入原始收件人地址和改写地址。

     一个电子邮件地址条目可能有多个改写条目，各个条目间使用空格分隔。域地址只能有 1 个改写条目。
   - 如果有现有的电子邮件或域地址改写条目文件，请勾选 **Email address or domain rewrite entry file（电子邮件地址或域改写条目文件）**复选框并浏览至该文件。文件大小不得超过 10 MB。
3. 单击 **OK（确定）**。您的条目将显示在 Envelope Recipient Address Rewrite List（信封收件人地址改写列表）中。

添加邮件头地址改写条目

使用 Inbound Messages（入站邮件）选项卡可以添加入站邮件的邮件头地址改写条目，使用 Outbound and Internal Messages（出站和内部邮件）选项卡可以添加出站或内部邮件地址掩蔽。Email Security 可以根据 Envelope Sender and Message Header Rewrite List（信封发件人和邮件头改写列表）来改写电子邮件信封发件人地址以及邮件头地址。

使用下列步骤添加地址改写条目:

1. 在 Envelope Sender and Message Header Rewrite List（信封发件人和邮件头改写列表）中单击 **Add（添加）**，打开 Add Sender Email or Domain Address（添加发件人电子邮件或域地址）页面。
2. 以下列两种方式之一输入地址:
   - 勾选 **Individual email address or domain rewrite entry（单个电子邮件地址或域改写条目）**复选框，并在相应的输入字段中输入原始发件人地址和改写地址。

     每个电子邮件或域地址条目只能有 1 个改写条目。
   - 如果有现有的电子邮件或域地址改写条目文件，请勾选 **Email address or domain rewrite entry file（电子邮件地址或域改写条目文件）**复选框并浏览至该文件。文件大小不得超过 10 MB。
3. 单击 **OK（确定）**。您的条目将显示在 Envelope Sender and Message Header Rewrite List（信封发件人和邮件头改写列表）中。

URL 沙盒

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

作为 Websense ThreatScope 的一个组件，URL 沙盒对嵌入在 Email Security 入站邮件中、未分类的 URL 提供了实时分析。当用户单击未分类的 URL 时，会显示一个着陆页，提示用户初始化 URL 分析。如果分析确定该链接为恶意链接，网站会被阻止。如果不是恶意链接，则用户会收到他们可以继续访问网站的通知。

您的订购必须包含 ThreatScope。仅当成功注册并启用电子邮件混合服务之后，URL 沙盒功能才可用。

URL 沙盒配置设置包括 3 个组成部分:

- 默认设置，应用于未涵盖在特定设置中的任何收件人
- 收件人特定设置，应用于个别域或电子邮件地址
- 不对其应用沙盒设置的域列表

使用 **Settings（设置）> Inbound/Outbound（入站 / 出站）> URL Sandboxing（URL 沙盒）**页面配置 ThreatScope URL 沙盒功能:

1. 在 Default Settings（默认设置）部分，指定应用于未涵盖在收件人特定设置中的任何收件人的设置。
   a. 勾选 **Analyze suspicious URLs（分析可疑 URL）**复选框，激活 URL 沙盒功能。默认情况下不勾选该复选框。
   b. 如果启用 URL 沙盒，则勾选 **Allow the recipient to follow links to unclassified URLs（允许收件人通过链接打开未分类的 URL）**复选框，允许用户单击未分类的 URL 链接。默认情况下不勾选该复选框。
   c. 勾选 **Allow the recipient to follow links with an unsupported protocol（允许收件人通过链接打开不支持的协议）**复选框，允许用户单击链接重定向到具有不支持的协议（例如，HTTPS）的网站。
   d. 如果想用其他文本替换原始 URL，请在复选框下方的输入字段中输入字符串。如果想显示原始 URL，请将该字段留空。
2. 使用 Recipient-specific Settings（收件人特定设置）区域，为单个域或电子邮件地址添加自定义沙盒设置。
   a. 单击 **Add（添加）**，为特定地址组创建沙盒设置。
   b. 在 Recipient Email/Domain Address List（收件人电子邮件 / 域地址列表）中，输入想要对其应用设置的逗号分隔的电子邮件或域地址。不允许使用通配符。
   c. 勾选 **Analyze suspicious URLs（分析可疑 URL）**复选框，为这些地址激活 URL 沙盒功能。默认情况下不勾选该复选框。
   d. 如果启用 URL 沙盒，则勾选 **Allow the recipient to follow links to unclassified URLs（允许收件人通过链接打开未分类的 URL）**复选框，允许指定用户单击未分类的 URL 链接。默认情况下不勾选该复选框。
   e. 勾选 **Allow the recipient to follow links with an unsupported protocol（允许收件人通过链接打开不支持的协议）**复选框，允许用户单击链接重定向到具有不支持的协议（例如，HTTPS）的网站。
   f. 如果想用其他文本替换原始 URL，请在复选框下方的输入字段中输入字符串。如果想显示原始 URL，请将该字段留空。
3. 如果即使 URL 所在的邮件里包含受信任发件人的数字签名，也要让沙盒检查 URL，那么请在 URL Sandbox（URL 沙盒）部分底部，勾选 **Analyze suspicious URLs that appear in digitally signed email（分析出现在含数字签名的电子邮件中的可疑 URL）**复选框。默认情况下不勾选该复选框。
4. 在复选框下面的输入字段中，输入您想要绕过 URL 沙盒的 URL 域。请勿使用通配符，并且要使用逗号分隔多个条目。

如果想要删除一组收件人特定设置，请勾选地址列表旁边的复选框，然后单击 **Delete（删除）**。

网络钓鱼检测和教育

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

网络钓鱼冒充可信实体，企图通过电子邮件获取个人信息（例如密码或信用卡号码）。例如，声称来自知名金融机构或流行网站的电子邮件实际上可能企图窃取个人信息。

Email Security Gateway 网络钓鱼检测功能是 Websense ThreatScope 的一部分。您的订购必须包含 ThreatScope，才能使用此功能。您必须已成功注册电子邮件混合服务，才能配置网络钓鱼检测和教育功能。

可以在云中针对网络钓鱼电子邮件的具体特征分析入站电子邮件。您可以定义规则来确定分析哪些发件人域，以及如何处理可疑的网络钓鱼电子邮件。可疑电子邮件可以按垃圾邮件处理（阻止并保存到垃圾邮件队列），或替换为教导收件人分辨网络钓鱼电子邮件的邮件。

仪表盘图表和演示报表可以配置为显示可疑网络钓鱼攻击数据。

Settings（设置）> Inbound/Outbound（入站 / 出站）> Phishing Detection（网络钓鱼检测）页面包含以下用于配置网络钓鱼检测的选项卡:

- **Phishing Rules（网络钓鱼规则）**，包含所有网络钓鱼规则列表。默认规则适用于不包括在任何其他定义规则中的域。有关信息，请参阅添加网络钓鱼检测规则（第 90 页）。

  无法删除默认规则。可以从列表中删除任何其他网络钓鱼规则，方法是勾选其关联的复选框并单击 **Delete（删除）**，然后单击 **Save to Cloud Service（保存到云服务）**。

- **Phishing Education Pages（网络钓鱼教育页面）**，包含您已定义的所有教育页面列表。如果未对网络钓鱼规则指定自定义页面，则应用默认页面。有关信息，请参阅创建网络钓鱼教育页面（第 91 页）。

  通过勾选相应复选框并单击 **Delete（删除）**，可从列表中删除任何网络钓鱼教育页面（默认页面除外）。您可能无法删除网络钓鱼规则正在使用的页面。

  仅当您收到有关与云服务同步问题的错误消息时，单击 **Save to Cloud Service（保存到云服务）**。

添加网络钓鱼检测规则

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用下列步骤配置网络钓鱼检测规则:

1. 单击 Phishing Rules（网络钓鱼规则）选项卡上的 **Add Rule（添加规则）**，可打开 Add Rule（添加规则）页面。
2. 在 **Phishing rule name（网络钓鱼规则名称）**输入字段输入规则的名称。

3. 在 **Domain names（域名）**输入字段中指定此网络钓鱼规则要应用的域。使用英文分号分隔多个域。
4. 为此网络钓鱼规则选择网络钓鱼操作选项:
   - **Treat as spam（视为垃圾邮件）**。隔离可疑的网络钓鱼邮件。
   - **Educate: Replace the URL with a link to the selected phishing education page and deliver the message.（教育：将 URL 更换为指向所选网络钓鱼教育页面的链接并传送邮件）**。
5. 针对网络钓鱼规则配置单个用户例外。例如，您可能想为特定用户或组选择不同的操作，或呈现不同的网络钓鱼教育页面。
   a. 单击 **Add User Exception（添加用户例外）**打开 Add User Exception（添加用户例外）对话框。
   b. 在 **Description（说明）**输入字段中输入此例外的简要说明。
   c. 在 **Email addresses（电子邮件地址）**输入字段中指定此例外要应用到的用户或组。
   d. 为此用户例外选择网络钓鱼操作选项:
      - **Treat as spam（视为垃圾邮件）**。隔离可疑的网络钓鱼邮件。
      - **Educate: Replace the URL with a link to the selected phishing education page and deliver the message.（教育：将 URL 更换为指向所选网络钓鱼教育页面的链接并传送邮件）**。
   e. 单击 **Add（添加）**。
6. 单击 **OK（确定）**以保存网络钓鱼规则。
7. 单击 Phishing Rules（网络钓鱼规则）选项卡中的 **Save to Cloud Service（保存到云服务）**，将网络钓鱼检测设置发送到电子邮件混合服务。

创建网络钓鱼教育页面

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

通过复制现有页面并重命名，可以创建新的网络钓鱼教育页面。也可以根据您的需求自定义默认邮件模板。如果未对网络钓鱼规则指定自定义页面，则使用默认页面。

使用下列步骤复制现有的网络钓鱼教育页面:

1. 单击 Phishing Education Pages（网络钓鱼教育页面）选项卡中的 **Copy Page（复制页面）**。
2. 在 **Page name（页面名称）**输入字段中输入网络钓鱼教育页面副本的名称。
3. 单击 **OK（确定）**。

使用下列步骤创建自定义网络钓鱼教育页面:

1. 单击 Phishing Education Pages（网络钓鱼教育页面）选项卡中的 **Add Page（添加页面）**选项卡，可打开 Add Phishing Education Page（添加网络钓鱼教育页面）屏幕。
2. 输入网络钓鱼教育页面的名称和说明。
3. 在 **Page title（页面标题）**字段中指定页面的标题。此标题显示为浏览器窗口名称。
4. 在 **Phishing Education Page Editor（网络钓鱼教育页面编辑器）**中指定所需的文本和图像。
5. 单击 **OK（确定）**。

> **注**
> 如果您收到有关与云服务同步问题的错误消息，应单击 Phishing Education Pages（网络钓鱼教育页面）选项卡中的 **Save to Cloud Service（保存到云服务）**，以将网络钓鱼教育页面设置发送到电子邮件混合服务。

管理邮件队列

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 **Main（主页）> Message Management（邮件管理）> Message Queues（邮件队列）**页面中可查看、创建和配置邮件队列。还可以修改以下默认队列:

- 病毒
- 垃圾邮件
- 异常
- 加密失败
- 解密失败
- 存档
- 安全加密

在 **Main（主页）> Message Management（邮件管理）> Blocked Messages（被阻止邮件）**页面中可以访问所有队列的所有被阻止邮件（有关详细信息，请参阅管理阻止的邮件队列）。在 **Main（主页）> Message Management（邮件管理）> Delayed Messages（延迟的邮件）**页面中可以查看临时延迟的邮件（相关信息请参阅管理延迟的邮件队列）。

邮件队列列表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Message Queues（邮件队列）页面的 Queue（队列）列表中包含关于每个队列的下列信息:

- 队列名称。单击队列列表中的队列名称可查看和管理队列中的邮件。有关详细信息，请参阅查看邮件队列（第 94 页）。
- 队列状态，指示队列是否在使用中。单击此列中的 **Referenced（已引用）**链接可查看正在使用该队列的 Email Security 功能列表。在队列移动操作过程中，此列中的图标指示移动正在进行或已失败。
- 邮件数量，指示该队列中的邮件总数。委托管理员可查看的邮件数可能少于此列中显示的总数，具体取决于授予该管理员的权限。
- 大小 / 总大小，指示队列当前大小占其最大配置大小的比例
- 存储位置，显示队列的存储位置（本地、通过网络文件系统 [NFS] 或通过 Samba）。此列中的图标指示存储状态，例如磁盘空间不足或失去连接。
- Properties（属性）列包含指向显示队列当前设置的页面的链接。单击此 **Edit（编辑）**链接可更改任何队列设置。

在队列列表中勾选队列名称旁边的复选框并单击 **Delete（删除）**，可删除用户创建的队列。默认队列无法删除。

相关主题:

- 创建邮件队列（第 93 页）
- 查看邮件队列（第 94 页）
- 管理阻止的邮件队列（第 96 页）
- 管理延迟的邮件队列（第 99 页）
- 查看队列中的邮件（第 100 页）

创建邮件队列

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用以下步骤在 **Main（主页）> Message Management（邮件管理）> Message Queues（邮件队列）**页面中创建新的邮件队列:

1. 单击队列列表下的 **Add（添加）**以打开 Add Queue（添加队列）页面。
2. 在 **Queue name（队列名称）**字段中输入新队列的名称。
3. 选择该队列的存储位置。
   - 使用 **Local（本地）**将队列存储在本机上。

- 选择 **Via Network File System (NFS)（通过网络文件系统 (NFS)）**使用 NFS 协议进行文件存储。输入存储位置的 IP 地址或主机名及其共享路径。

  注
  Email Security Gateway 支持使用 NFS 版本 3 或更高版本。

- 选择 **Via Samba（通过 Samba）**以使用 Samba 进行文件存储。为 Samba 输入下列信息:
  - 存储位置的 IP 地址或主机名
  - 其共享路径
  - 用户名
  - 密码

4. 在 **Maximum message retention（邮件保留最大天数）**字段中配置邮件在队列中保留的最大天数（从 1 至 180 天）。默认队列的默认保留天数为 180 天，管理员创建的队列的保留天数为 30 天。
5. 配置最大队列大小（从 1 至 51200 MB），默认值为 1024。
6. 对于集群中的设备，指定分配给每个集群机器的最大存储大小（单位为 MB）。

更改邮件队列属性

要更改邮件队列的属性，请在该队列的 Queue List Properties（队列列表属性）列中单击 **Edit（编辑）**以打开 Edit Queue（编辑队列）页面。

查看邮件队列

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 Message Queues（邮件队列）页面的 Queue（队列）列表中单击队列名称以打开该队列。使用 **View from/to（查看从 / 至）**字段可指定要查看的条目的日期 / 时间范围。日历包括以下选项:

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。单击 **View（查看）**日期 / 时间范围右侧的箭头以显示需要的队列项。

还可以对邮件队列执行关键字搜索，或者通过指定仅搜索发件人、收件人、主题或应用策略，进一步缩小搜索范围。还可以搜索处理邮件的设备名称（Processed By（处理设备）类别）。输入关键字并单击 **Search（搜索）**。

在 **per page（每页）**下拉列表中，配置要在队列的每页中查看的邮件数量（25 [默认值]、50 或 100）。

邮件列表中显示的信息包括以下各项:

- 发件人电子邮件地址
- 收件人电子邮件地址
- 邮件主题。通过单击 Subject（主题）列中的链接以打开 View Message（查看邮件）页面，可查看邮件信息和邮件内容。请参阅查看队列中的邮件（第 100 页）。
- 邮件大小
- 收到邮件的日期 / 时间
- 对邮件应用的策略和规则。如果对邮件应用了 Data Security 策略，**View Incident（查看事件）**链接将打开处理该邮件的 Data Security 中的数据泄露防护事件信息。

  存档队列不显示该列。
- 邮件类型（例如垃圾邮件、病毒、异常、商业群发电子邮件、ThreatScope、加密错误或解密错误）
- 处理邮件的设备名称，包括在 **Processed By（处理设备）**列中。
- **Reason for Quarantine（隔离原因）**列包含一个指示邮件为什么会被送到隔离队列的条目:

列条目	隔离触发者
AV（防毒软件）	防病毒过滤器
HYBRID（混合应用）	电子邮件混合服务
ASA_URL	URL 扫描过滤器
ASA_BATV_SPAM	退信地址标记验证
ASA_DFP	数字指纹防垃圾邮件工具
ASA_LEXIRULES	LexiRules 防垃圾邮件工具
ASA_HEURISTICS	Heuristics 防垃圾邮件工具
Commercial Bulk（商业群发电子邮件）	商业群发电子邮件过滤器
Custom Content（自定义内容）	自定义内容过滤器
Block List（阻止列表）	Personal Email Manager 始终阻止列表条目
Archive（存档）	存档功能（**Settings（设置）> Inbound/Outbound（入站 / 出站）> Message Control（邮件控制）**设置）
Exception（异常）	邮件异常

您可以选择队列中的邮件并执行以下操作:

操作	说明
Deliver（传送）	将邮件传送到收件人。
Delete（删除）	从队列中删除邮件。
Reprocess（重新处理）	从队列中删除邮件并重新启动电子邮件处理功能（如同 Email Security 首次接收它）。对于存档队列，此操作称为 **Process（处理）**。
Not Spam（非垃圾邮件）	报告该邮件不应归类为垃圾邮件并允许传送该邮件。仅在选择了垃圾邮件时，此选项才可用。
Refresh（刷新）	刷新队列内容列表以查看最新的队列内容。

More Actions（更多操作）下拉列表包括以下操作:

操作	说明
Resume Processing（恢复处理）	具有垃圾邮件和病毒特性的邮件在被其他类型过滤器处理之前，可能被一种类型的过滤器隔离。如果最初隔离为误报，使用此操作可确保邮件被所有相关的过滤器处理，而不是在第一次扫描后就传送。
Add to Always Block List（添加到始终阻止列表）	将邮件发件人添加到 Always Block（始终阻止）列表。
Add to Always Permit List（添加到始终允许列表）	将邮件发件人添加到 Always Permit（始终允许）列表。
Forward（转发）	将邮件转发到一个或多个收件人。转发的邮件作为附件添加到转发邮件。
Download（下载）	以 .eml 格式下载邮件。下载的电子邮件将保存为 zip 文件。
Clear message queue（清除邮件队列）	删除队列中的所有邮件。
Reprocess all messages（重新处理所有邮件）	重新处理搜索结果中的所有邮件。Email Security Gateway 仅会重新处理搜索结果中的前 5000 个条目。
Delete all messages（删除所有邮件）	删除搜索结果中的所有邮件。Email Security Gateway 仅会删除搜索结果中的前 5000 个条目。

管理阻止的邮件队列

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Main（主页）> Message Management（邮件管理）> Blocked Messages（被阻止邮件）页面将所有设备多数队列中的所有被阻止邮件列在单个表格中，并包含一个指示存储邮件的队列名称的列条目。存档和 Delayed Messages（延迟的邮件）队列中的邮件不包括在该页面。

使用 **View from/to（查看从 / 至）**字段可指定要查看的条目的日期 / 时间范围。日历包括以下选项:

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。单击 **View（查看）**日期 / 时间范围右侧的箭头以显示需要的队列项。

还可以对所有被阻止邮件执行关键字搜索，或者通过指定仅搜索发件人、收件人、主题或应用策略，进一步缩小搜索范围。还可以搜索单个队列或处理邮件的设备名称（Processed By（处理设备）类别）。输入关键字并单击 **Search（搜索）**。

在 **per page（每页）**下拉列表中，配置要在队列的每页中查看的邮件数量（25 [默认值]、50 或 100）。

邮件列表中显示的信息包括以下各项:

- 发件人电子邮件地址
- 收件人电子邮件地址
- 邮件主题。通过单击 Subject（主题）列中的链接以打开 View Message（查看邮件）页面，可查看邮件信息和邮件内容。请参阅查看队列中的邮件（第 100 页）。
- 邮件大小
- 收到邮件的日期 / 时间
- 对邮件应用的策略和规则。如果对邮件应用了 Data Security 策略，**View Incident（查看事件）**链接将打开处理该邮件的 Data Security 中的数据泄露防护事件信息。
- 队列名称（例如垃圾邮件、病毒、异常、加密失败或解密失败）
- 邮件类型（例如垃圾邮件、病毒、异常、商业群发电子邮件、加密错误或解密错误）
- 处理邮件的设备名称，包括在 **Processed By（处理设备）**列中。
- **Reason for Quarantine（隔离原因）**列包含一个指示邮件为什么会被送到隔离队列的条目:

列条目	隔离触发者
AV（防毒软件）	防病毒过滤器
HYBRID（混合应用）	电子邮件混合服务
ASA_URL	URL 扫描过滤器
ASA_BATV_SPAM	退信地址标记验证

列条目	隔离触发者
ASA_DFP	数字指纹防垃圾邮件工具
ASA_LEXIRULES	LexiRules 防垃圾邮件工具
ASA_HEURISTICS	Heuristics 防垃圾邮件工具
Commercial Bulk（商业群发电子邮件）	商业群发电子邮件过滤器
Custom Content（自定义内容）	自定义内容过滤器
Block List（阻止列表）	Personal Email Manager 始终阻止列表条目
Archive（存档）	存档功能（**Settings（设置）> Inbound/Outbound（入站 / 出站）> Message Control（邮件控制）**设置）
Exception（异常）	邮件异常

您可以选择被阻止邮件队列中的邮件并执行以下操作:

操作	说明
Deliver（传送）	将邮件传送到收件人。
Delete（删除）	从队列中删除邮件。
Reprocess（重新处理）	从队列中删除邮件并重新启动电子邮件处理功能（如同 Email Security 首次接收它）。
Not Spam（非垃圾邮件）	报告该邮件不应归类为垃圾邮件并允许传送该邮件。仅在选择了垃圾邮件时，此选项才可用。
Refresh（刷新）	刷新队列内容列表以查看最新的队列内容。

More Actions（更多操作）下拉列表包括以下操作:

操作	说明
Resume Processing（恢复处理）	具有垃圾邮件和病毒特性的邮件在被其他类型过滤器处理之前，可能被一种类型的过滤器隔离。如果最初隔离为误报，使用此操作可确保邮件被所有相关的过滤器处理，而不是在第一次扫描后就传送。
Add to Always Block List（添加到始终阻止列表）	将邮件发件人添加到 Always Block（始终阻止）列表。
Add to Always Permit List（添加到始终允许列表）	将邮件发件人添加到 Always Permit（始终允许）列表。
Forward（转发）	将邮件转发到一个或多个收件人。转发的邮件作为附件添加到转发邮件。
Download（下载）	以 .eml 格式下载邮件。下载的电子邮件将保存为 zip 文件。

操作	说明
Reprocess all messages（重新处理所有邮件）	重新处理搜索结果中的所有邮件。Email Security Gateway 仅会重新处理搜索结果中的前 5000 个条目。
Delete all messages（删除所有邮件）	删除搜索结果中的所有邮件。Email Security Gateway 仅会删除搜索结果中的前 5000 个条目。

管理延迟的邮件队列

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

因各种连接问题暂时无法传送的电子邮件被发送到延迟的邮件队列中。延迟的邮件可能会被系统自动重新发送。有关设置延迟邮件的传送重试间隔和配置针对无法传送的邮件而发送的通知邮件的信息，请参阅处理未传送的邮件（第 102 页）。

也可以使用自定义内容过滤器操作计划在未来的日期传送延迟的邮件。有关自定义内容过滤器的信息，请参阅自定义内容（第 112 页）；有关计划延迟邮件传送的详细信息，请参阅创建和配置过滤器操作（第 122 页）。

可以在 **Main（主页）> Message Management（邮件管理）> Delayed Messages（延迟的邮件）**页面中查看此队列中的邮件和手动执行所需的处理活动。当 Delayed Messages（延迟的邮件）页面出现时，将显示最近的邮件。使用 **View from/to（查看从 / 至）**字段可指定要查看的邮件的日期 / 时间范围。日历包括以下选项:

- 使用日历顶部年和月旁边的上一页和下一页箭头可更改年份和月份。
- 单击日历左下角的日期可将日历设置为当前日期。
- 单击 **Clean（清除）**以清除当前日期 / 时间日历选择。
- 单击 **Today（今天）**以设置日历日期为今天日期。

在日历右侧的输入字段中设定小时及分钟范围。单击 **View（查看）**日期 / 时间范围右侧的箭头以显示需要的队列项。

还可以对邮件队列执行关键字搜索，或者通过指定仅搜索发件人、收件人或主题，进一步缩小搜索范围。如果设备配置在集群中，还可以搜索处理邮件的设备的名称。输入关键字并单击 **Search（搜索）**。

可在队列列表横幅的 **Per page（每页）**下拉列表中配置每页的邮件数量（25 与 100 之间，包括 25 [默认值]、50 或 100）。

邮件列表中显示的信息包括以下各项:

- 发件人电子邮件地址
- 收件人电子邮件地址
- 邮件主题。通过单击 Subject（主题）列中的链接以打开 View Message（查看邮件）页面，可查看邮件信息和邮件内容。请参阅查看队列中的邮件（第 100 页）。

- 邮件大小
- 收到邮件的日期 / 时间
- 对邮件应用的策略和规则。如果对邮件应用了 Data Security 策略，**View Incident（查看事件）**链接将打开处理该邮件的 Data Security 中的数据泄露防护事件信息。
- 计划下一次邮件传送尝试的日期
- 邮件被延迟的原因。该列中的条目可能为下列选项之一:
  - Temporary connection issue delay *n*（临时连接问题延迟 *n*）。由于连接问题导致的临时延迟； *n* 为邮件剩余的重试次数。
  - Scheduled delay（计划的延迟）。通过自定义内容过滤器操作计划的有意延迟（有关信息，请参阅创建和配置过滤器操作（第 122 页））。
  - ThreatScope analysis delay（ThreatScope 分析延迟）。由于正在进行文件沙盒分析而导致的暂时性延迟。
- 处理邮件的设备名称，包括在 **Processed By（处理设备）**列中。

您可以选择队列中的邮件并执行以下操作:

操作	说明
Release（释放）	立即尝试邮件传送。
Delete（删除）	从队列中删除邮件。
Refresh（刷新）	刷新队列内容列表以查看最新的队列内容。

More Actions（更多操作）下拉列表包括以下操作:

操作	说明
Forward（转发）	将邮件转发到一个或多个收件人。转发的邮件作为附件添加到转发邮件。
Download（下载）	以 .eml 格式下载邮件。下载的电子邮件将保存为 zip 文件。
Release all messages（释放所有邮件）	尝试传送队列中的所有邮件。
Delete all messages（删除所有邮件）	删除搜索结果中的所有邮件。Email Security Gateway 仅会删除搜索结果中的前 5000 个条目。

查看队列中的邮件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在队列的 Subject（主题）列中单击邮件的链接以打开 View Message（查看邮件）页面，该页面包含邮件的详细信息以及邮件内容。页面顶部的 **Back（返回）**链接用于返回到 View Queue（查看队列）页面。**Previous（上一个）**和 **Next（下一个）**链接用于导航到队列邮件列表中的上一个或下一个邮件。

View Message（查看邮件）页面显示关于所选邮件的下列信息:

字段名称	说明
Sender（发件人）	发件人的电子邮件地址
Recipient（收件人）	收件人的电子邮件地址
From（自）	发件人的名称
To（至）	收件人的名称
Date（日期）	收到邮件的日期
Policy（策略）	应用于邮件的策略名称
Message type（邮件类型）	邮件类型，指示邮件分析结果（安全、病毒、垃圾邮件、数据使用、异常、商业群发电子邮件、网络钓鱼或自定义内容）
Processed by（处理设备）	处理邮件的设备的名称
Header（邮件头）	单击该链接可查看邮件头
Attachment（附件）	如果该邮件包含附件，则通过该链接可打开附件。
Subject（主题）	邮件主题

适用于任何 View Queue（查看队列）页面的邮件操作也适用于 View Message（查看邮件）页面，Clear All Messages（清除所有邮件）或 Release All Messages（释放所有邮件）除外。有关这些操作的说明，请参阅查看邮件队列（第 94 页）。还可以选择以文本格式或 HTML 格式查看邮件内容，或 **Clear message queue（清除邮件队列）**，这些选项位于 More Actions（更多操作）下拉列表中。

配置邮件异常设置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Settings（设置）> Inbound/Outbound（入站 / 出站）> Exceptions（异常）页面指定在 Email Security Gateway 中如何处理因某些原因而无法处理的邮件。配置邮件异常设置如下:

1. 指定对 Email Security Gateway 无法处理的邮件要执行的操作:
   - 如果异常由防病毒过滤器造成，则传送邮件。
   - 如果异常由防垃圾邮件过滤器造成，则传送邮件（默认设置）。
   - 如果异常由 ThreatScope 过滤器造成，则传送邮件（默认设置）。
   - 如果异常由商业群发电子邮件过滤器造成，则传送邮件。
   - 如果异常由 Data Security 造成，则传送邮件（默认设置）。
   - 如果异常由任何其他 Email Security Gateway 操作造成，则传送邮件。

- 将异常邮件保存到队列（默认设置）。

  从下拉列表中选择所需的文件夹（默认为 **exception（异常）**）。该列表包括所有默认队列的名称和管理员创建的队列。如果要添加新队列，请从下拉列表中选择 **Add Folder（添加文件夹）**以打开 Add Queue（添加队列）屏幕。

  警告

  要将无法传送的邮件保存到队列，必须选择保存选项。如果未选择此选项，邮件可能会从 Email Security Gateway 断开连接。

2. 如果要发送关于未处理邮件的通知，请勾选 **Send notification（发送通知）**复选框以启用 Notification Properties（通知属性）部分。
3. 从以下选项指定通知邮件发件人:
   - Original email sender（原始邮件发件人）（默认选择）
   - Administrator（管理员）。如果使用此选项，您必须在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面中配置有效的管理员电子邮件地址（请参阅设置系统通知电子邮件地址（第 50 页））。
   - Custom（自定义）。在此字段中指定一个电子邮件地址。
4. 从以下选项指定一个或多个通知邮件收件人:
   - Original email sender（原始电子邮件发件人）
   - Original email recipient（原始电子邮件收件人）
   - Administrator（管理员）（默认选择）。如果使用此选项，您必须在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面中配置有效的管理员电子邮件地址（请参阅设置系统通知电子邮件地址（第 50 页））。
   - User specified（用户指定）。在此字段中输入一个或多个电子邮件地址，用分号分隔。
5. 在 **Subject（主题）**字段中指定通知邮件的主题行。
6. 在 **Content（内容）**字段中输入通知邮件的正文。
7. 如果要将原始邮件附加到通知邮件，请勾选 **Attach original message（附加原始邮件）**复选框。

处理未传送的邮件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

邮件传送选项可帮助您控制如何处理无法传送的邮件。这些操作的相关选项显示在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Undelivered Options（未传送选项）**页面中。

使用以下步骤确定如何处理由于错误情况暂时无法传送的邮件:

1. 在 Undelivered Message Options（未传送的邮件选项）部分的 **Retry interval（重试间隔）**字段中，输入邮件重试间隔的时间（单位为分钟）。

   重要事项

   Email Security Gateway 以指数方式计算邮件传送重试间隔。例如，使用默认项 15 分钟，则重试间隔为 15 分钟、30 分钟、60 分钟、120 分钟、240 分钟，以此类推。

2. 在 **Maximum retry period（最大重试时间间隔）**字段中，输入重试邮件传送的最大时间段（单位为分钟，默认值为 1440）。
3. 在 **Notification email address（通知电子邮件地址）**字段中，输入您要向其发送通知（在重试周期结束时未送达报表 (NDR) 无法传送给原始发件人）的电子邮件地址。

   勾选 **Use Administrator email address（使用管理员电子邮件地址）**复选框以发送这些邮件到管理员。您必须在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面中配置管理员地址（请参阅设置系统通知电子邮件地址（第 50 页））。

流量整形选项

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Traffic Shaping（流量整形）**屏幕上，可以为基于域组或用户目录设置的指定来源或目的地组确定流量传送的速率。例如，通过这些设置，您能以一定的速率发送大量的电子邮件，并且在该速率下可防止域被列入黑名单。

通过勾选相应复选框并使用 **Move Up（上移）**和 **Move Down（下移）**按钮，可更改流量整形组的顺序。通过勾选相应复选框并单击 **Copy（复制）**，可复制现有的流量整形组。通过勾选相应复选框并单击 **Delete（删除）**，可删除流量整形组。

除指定来源和目的地用户组以外，还可以在设置流量整形时修改以下邮件传送设置:

- 最大并发连接数
- 指定时间段内每个连接的最大邮件数量
- 每封邮件的最大收件人数量
- 使用 SMTP 会话缓存，为其指定每个会话的最大邮件数量和会话持续时间

默认的流量整形组不包含任何流量来源或目的地用户组。

单击 **Add（添加）**并使用以下步骤，在您的系统中建立邮件流量整形控制。

1. 为您的流量整形组添加名称。
2. 在 **Order（顺序）**列表中选择该组，指定您想让其出现在流量整形组列表中的位置。
3. 选择流量整形组的状态：**Active（活动）**或 **Disabled（禁用）**。
4. 如需要，配置电子邮件来源流量整形组。指定以下其中 1 个来源类型:
   - All sources（所有来源）
   - Domain group（域组）（默认选择）。从下拉列表中选择域组。单击 **Edit（编辑）**，修改所选择的域组。
   - User directory（用户目录）。从列表中选择用户目录，或单击 **Add user directory（添加用户目录）**，新建用户目录。
5. 如需要，配置电子邮件目的地流量整形组。指定以下其中 1 个目的地类型:
   - All destinations（所有目的地）
   - Domain group（域组）（默认选择）。从下拉列表中选择域组。单击 **Edit（编辑）**，修改所选择的域组。
   - User directory（用户目录）。从列表中选择用户目录，或单击 **Add user directory（添加用户目录）**，新建用户目录。
6. 在 **Maximum number of concurrent connections（最大并发连接数）**字段中，输入同时传送邮件到单个路由地址的最大数量。值的范围为 5 - 50，默认值为 20。
7. 在 **Maximum number of messages per connection（每个连接的最大邮件数量）**字段中，输入定义的时间段内每个连接的最大邮件数量。邮件数量范围为 1 - 10000；默认值为 10000。时间范围为 60 秒到 30 分钟；默认值为 60 秒。
8. 在 **Maximum number of recipients（最大收件人数量）**字段中，输入每次邮件传送的最大收件人数量。值的范围为 5 - 100，默认值为 50。
9. 如果要使用 SMTP 会话缓存，请勾选 **Enable SMTP session cache（启用 SMTP 会话缓存）**复选框（默认设置）。
   a. 指定每个 SMTP 会话允许的最大邮件数量。值的范围为 5 - 100；默认值为 10。可以输入零 (0)，以指定每个会话邮件数量不受限制。
   b. 指定 SMTP 会话的持续时间，以秒为单位。值的范围为 60 - 600 秒，默认值为 300 秒。

处理加密的邮件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 Data Security 模块中配置的电子邮件内容策略可能指定邮件应加密传送。如果您要对特定出站邮件进行加密，则必须在 Data Security 管理器中创建包括加密操作计划在内的电子邮件 DLP 策略（**Main（主页）> Policy Management（策略管理）> DLP Policies（DLP 策略）**）。

Email Security Gateway 支持以下类型的邮件加密:

- *安全邮件传送*
- *强制性的传输层安全性 (TLS) 加密*
- *高级电子邮件加密*
- *第三方加密应用程序*

使用 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Encryption（加密）**页面指定 Email Security Gateway 使用的加密类型。

安全邮件传送

安全邮件传送是一种本地加密方法，可让您为安全门户配置传送选项，组织客户可以通过安全门户查看、发送和管理加密的电子邮件。例如，您可能希望在发送给客户的邮件中包含敏感的个人金融信息。该门户提供安全位置来传输此数据。

您组织内可发送和接收安全邮件的用户可通过其本地电子邮件客户端（而不是安全门户）来处理这些邮件。

安全邮件存储在默认的安全加密队列中（**Main（主页）> Message Management（邮件管理）> Message Queues（邮件队列）**）。您可以在安全加密队列视图中搜索和删除邮件。可能无法查看邮件详细信息。在 Edit Queue（编辑队列）页面中配置最大队列大小和邮件保留天数。

从 **Encryption method（加密方法）**下拉列表中选择 **Secure Message Delivery（安全邮件传送）**以显示安全邮件选项，包括用户收到的以提醒其加密邮件的通知模板。选择此选项时，Email Security Gateway 其他加密方法不可用。

使用下列步骤配置安全邮件传送加密:

1. 输入托管安全邮件传送门户的设备的 IP 地址或主机名（主机名的最大长度为 64 个字符）。

   建议输入主机名而不是 IP 地址，以避免通知邮件在最终用户的收件箱中生成潜在的 Microsoft Outlook 警告邮件。

   重要事项

   该字段中的输入应映射到 E1 接口（面向 V10000 G2/G3 设备）或 P1 接口（面向 V5000 G2 设备）。确保您使用的接口从内部网络之外可见。

   如果您有设备集群，请输入 1 个集群设备（主要或次要）的 IP 地址或主机名。集群负载均衡功能适当地定向流量。

   注

   安全邮件使用为 Personal Email Manager 门户配置的同一端口（**Settings（设置）> Personal Email（个人电子邮件）> Notification Message（通知邮件）**）。

2. 指定允许您的用户在安全门户执行的操作，以及这些用户可向其发送安全邮件的收件人的类型:

   - **Maximum message size（最大邮件大小）**。客户邮件大小包括任何附件。默认值为 50 MB；最大值为 100 MB。
   - **Reply all to secure messages received in the portal**（全部回复门户中收到的安全邮件）。客户可以回复所有收件人。但是，如果为 Allowed Recipients（允许收件人）选择 **Internal domain email addresses only（仅内部域电子邮件地址）**选项，则用户仅可回复您组织内的收件人。

     无法为此类型的邮件修改收件人列表。
   - **Forward secure messages received in the portal**（转发门户中收到的安全邮件）。客户可以将收到的任何安全邮件转发给允许的收件人。
   - **Compose new secure messages within the portal**（在门户内撰写新的安全邮件）。客户可以撰写新的安全邮件并将其发送给允许的收件人。
   - **Attach files to secure messages sent from the portal（向从门户发送的安全邮件附加文件）**。客户可在安全邮件中发送附件。

   默认情况下会选中所有上述选项。

Allowed Recipients（允许收件人）框提供您的客户可向其回复、转发或发送新安全邮件的收件人的类型选项。出于安全目的，收件人列表必须至少包括您组织内的一个电子邮件地址。

- **Internal domain email addresses only（仅内部域电子邮件地址）**。仅组织受保护域内部的电子邮件地址可以指定为收件人。
- **Internal and external domain email addresses (at least one internal email address required)（内部和外部域电子邮件地址（至少需要一个内部电子邮件地址））**。组织受保护域外部的电子邮件地址可以指定为收件人，但必须至少输入域内部的 1 个地址（默认选择）。

  有关确定受保护域的详细信息，请参阅受保护域组（第 59 页）。

Secure Email End-User Notification（安全电子邮件最终用户通知）区域包含发送给用户的安全邮件已发送到门户以供查看时用户收到的电子邮件的邮件模板。使用默认模板，或根据您的需求自定义模板。您必须在通知中包括 URL 字段，因为这可创建允许您的客户访问安全电子邮件门户的链接。

在 **Sender（收件人）**字段中输入通知的 1 个发件人地址，并在 **Subject（主题）**字段中指定电子邮件主题。发件人地址必须属于您的内部受保护域。由于您不希望对通知作出响应，请确保将发件人地址配置为放弃对此通知作出任何直接回复。

配置您的通知邮件后，单击 **Preview Message（预览邮件）**以查看它。

门户可显示为 9 个语言版本，用户可在注册过程中选择一种语言。Websense 技术文档库中提供了 Websense Secure Messaging 用户帮助，其也有 9 个语言版本。它介绍了用户注册过程以及如何使用安全邮件门户。

强制性的传输层安全性 (TLS) 加密

TLS 是一种为所有电子邮件传输（入站、出站和内部）提供安全性的 Internet 协议。客户端和服务器针对要发生的传输协商一种安全可靠的“握手”连接（只要客户端和服务器支持相同版本的 TLS）。

在 Email Security 中，如果只选择 TLS 进行邮件加密，并且客户端和服务器无法协商安全的 TLS 连接，则邮件被发送到延迟的邮件队列中，以供以后尝试传送。在 **Encryption method（加密方法）**下拉列表中选择 **Transport Layer Security (TLS)（传输层安全性 (TLS)）**，并选择 **Use TLS only (no backup encryption method; message is queued for later delivery attempt)（仅使用 TLS（没有备用加密方法；邮件置于队列中以供以后尝试传送））**选项，以仅使用 TLS 进行邮件加密。

如果选择 TLS 进行邮件加密，您可以指定高级电子邮件加密或第三方应用程序作为备用方法，以防 TLS 连接失败。指定备用选项允许在 TLS 连接不成功的情况下还有机会进行邮件加密。如果 TLS 和备用连接都不成功，则邮件被发送到延迟的邮件队列中，以供以后尝试连接。

在 **Encryption method（加密方法）**下拉列表中选择 **Transport Layer Security (TLS)（传输层安全性 (TLS)）**选项以启用 TLS 加密。然后勾选以下选项中的 1 个，以启用备用加密方法:

- **Use Advanced Email Encryption as backup encryption method（使用高级电子邮件加密作为备用加密方法）**
- **Use third-party application as backup encryption method（使用第三方应用程序作为备用加密方法）**

有关这些加密方法的信息，请参阅高级电子邮件加密（第 108 页）和第三方加密应用程序（第 109 页）。

高级电子邮件加密

如果要使用混合服务对出站邮件执行加密，请在 **Encryption method（加密方法）**下拉列表中选择 **Advanced Email Encryption（高级电子邮件加密）**选项。仅当您的订购包括电子邮件混合服务，且混合服务已注册并启用时，高级邮件加密才可用。

如果选择了强制性 TLS 加密，还可以指定高级邮件加密为备用加密方法。有关详细信息，请参阅强制性的传输层安全性 *(TLS)* 加密（第 107 页）。

在 Data Security 策略标识出站邮件需要加密时，该邮件通过 TLS 连接发送到混合服务。如果未建立安全连接，则将该邮件置于延迟的邮件队列中，以供以后尝试传送。

用于将电子邮件发送到混合服务进行加密的 SMTP 服务器地址在混合服务设置过程中配置。使用 **Settings（设置）> Hybrid Service（混合服务）> Hybrid Configuration（混合配置）**下的 Delivery Route（传送路由）页面添加出站 SMTP 服务器地址（请参阅指定传送路由（第 37 页））。

如果混合服务在加密的出站邮件中检测到垃圾邮件或病毒，则将邮件退回到该邮件的发件人。

混合服务尝试解密入站加密邮件，并向邮件添加 x-header 以指示解密操作是否成功。无论邮件解密是否成功，都会执行邮件分析。

混合服务不对入站或内部邮件进行加密。必须修改 Data Security 策略，以指定在使用混合服务时只对出站邮件进行加密。

在 Websense 技术文档库的 Websense Email Security Gateway 加密中查找有关高级电子邮件加密的详细信息。

第三方加密应用程序

Email Security Gateway 支持使用第三方软件进行电子邮件加密。所用的第三方应用程序必须支持使用 x-header 与 Email Security 通信。

如果选择了强制性 TLS 加密，还可以指定第三方应用程序加密为备用加密方法。有关详细信息，请参阅强制性的传输层安全性 *(TLS)* 加密（第 107 页）。

可配置 Email Security Gateway 将触发 Data Security 加密策略的 x-header 添加到邮件中。其他 x-header 用于指示加密成功或失败。这些 x-header 有助于 Email Security Gateway 与加密软件之间的通信。必须确保 Email Security Gateway 加密页面中的 x-header 设置与第三方软件配置中的对应设置相匹配，以便 Email Security 能够与第三方软件通信。

Email Security Gateway x-header 设置在 **Settings（设置）> Inbound/Outbound（入站 / 出站）> Encryption（加密）**页面中输入。在 **Encryption method（加密方法）**下拉列表中选择 **Third party application（第三方应用程序）**，以配置 Email Security 使用外部加密软件。使用以下步骤在 Email Security Gateway 中配置第三方应用程序加密:

1. 添加加密服务器（最大 32 个）到 Encryption Server List（加密服务器列表）：
   a. 输入每个服务器的 IP 地址或主机名和端口号。
   b. 如果要使用 MX 查找功能，请勾选 **Enable MX lookup（启用 MX 查找）**复选框。
   c. 单击 Add Encryption Server（添加加密服务器）框右边的箭头，将服务器添加到 Encryption Server List（加密服务器列表）。

   如果要从列表中删除服务器，请选择它并单击 **Remove（删除）**。
2. 在 **Encrypted IP address group（加密的 IP 地址组）**下拉列表中，指定 IP 地址（如果启用了解密或将加密的电子邮件配置为返回到 Email Security）。默认为加密网关。
3. 如果要用户提供凭证才能查看加密的邮件，请勾选 **Require authentication（需要身份验证）**复选框，并在相应的字段提供所需的用户名和密码。加密服务器必须支持并配置身份验证才能使用此功能。
4. 在 **Encryption X-Header（加密 X-Header）**字段中，指定要添加到应加密邮件中的 X-Header。还必须在加密服务器上设置并启用该 X-Header 的值。
5. 在 **Encryption Success X-Header（加密成功 X-Header）**字段中，指定要添加到已成功加密的邮件中的 X-Header。还必须在加密服务器上设置并启用该 X-Header 的值。

6. 在 **Encryption Failure X-Header（加密失败 X-Header）**字段中，指定要添加到加密失败的邮件中的 X-Header。还必须在加密服务器上设置并启用该 X-Header 的值。
7. 选择任何所需的加密失败选项:
   - 如果要将邮件隔离到某个队列中，请勾选 **Isolate messages to queue（隔离邮件到队列）**复选框。从下拉列表中选择隔离邮件的队列（默认为病毒队列）。
   - 如果要发送通知到原始发件人，请勾选 **Send notification to original sender（发送通知到原始发件人）**复选框。

     在 Notification Details（通知详细信息）部分的相应字段中输入通知邮件的主题和内容。如果要将原始邮件作为附件附加到通知邮件，请勾选 **Attach original message（附加原始邮件）**复选框。
   - 如果要传送加密操作失败的邮件，请选择 **Deliver message（传送邮件）**（默认）。
   - 如果不想传送加密操作失败的邮件，请选择 **Drop message（放弃邮件）**。
8. 如果需要 Email Security 解密已加密的邮件，请勾选 **Enable decryption（启用解密）**复选框。
9. 选择任何所需的解密选项:
   - 在 **Content type（内容类型）**字段中，输入要解密的邮件内容类型，多个类型之间用分号分隔。最大长度为 49 个字符。默认条目包括 multipart/signed、multipart/encrypted 和 application/pkcs7-mime。
   - 在 **X-Header** 字段中，指定标识待解密邮件的邮件 x-header。还必须在加密服务器上设置并启用该 X-Header 的值。
   - 在 **Decryption X-Header（解密 X-Header）**字段中，指定要添加到应解密邮件中的 X-Header。还必须在加密服务器上设置并启用该 X-Header 的值。
   - 在 **Decryption Success X-Header（解密成功 X-Header）**字段中，指定要添加到已成功解密的邮件中的 X-Header。还必须在加密服务器上设置并启用该 X-Header 的值。
   - 在 **Decryption Failure X-Header（解密失败 X-Header）**字段中，指定要添加到解密失败的邮件中的 X-Header。还必须在加密服务器上设置并启用该 X-Header 的值。
   - 如果要将解密失败的邮件转发到特定的队列，请勾选 **On decryption failure（解密失败队列）**复选框，然后从下拉列表中选择这些邮件的队列（默认为病毒队列）。

5 使用过滤器和策略

主题:

管理过滤器

Email Security Gateway 具有以下预定义的默认过滤器类型：病毒、URL 扫描、垃圾邮件、商业群发电子邮件、Websense ThreatScope 以及免责声明。病毒过滤器可分析邮件及其附件是否存在病毒和其他威胁。URL 扫描检测电子邮件内容中的嵌入式 URL 并根据已知垃圾邮件 URL 数据库将其归类。垃圾邮件过滤器可扫描电子邮件内容并将其与已知垃圾邮件特征的数据库进行比较。有许多防垃圾邮件工具可供选择，包括数字指纹、LexiRules 以及启发式扫描工具。商业群发电子邮件过滤器会对邮件进行分析，确定该邮件是否为企业所发，用于广告目的。ThreatScope 过滤器会检测通常含有安全威胁的电子邮件附件文件类型（包括 .exe、.pdf、.xls、.xlsx、.doc、.docx、.ppt、.pptx，以及存档文件）。如果要在邮件的开头或结尾添加文本，请使用免责声明过滤器。

也可根据您配置的邮件组件条件创建自定义内容过滤器来扫描邮件。Email Security 不提供默认的自定义内容过滤器。

过滤器通过 **Main（主页）> Policy Management（策略管理）> Filters（过滤器）** 页面创建和管理。单击 **Add（添加）** 打开 Add Filter（添加过滤器）页面并设置新过滤器的属性（请参阅创建和配置过滤器（第 112 页））。

还可以复制过滤器，无论其是否被策略使用。可删除未被任何策略使用的过滤器。但是 Email Security 的默认过滤器无法复制或删除。

复制过滤器

通过勾选过滤器名称左侧的复选框并单击 **Copy（复制）**，可复制现有过滤器。在 Copy Filter（复制过滤器）对话框中输入新过滤器名称，然后单击 **OK（确定）**。单击 Filters（过滤器）列表中的新过滤器名称以打开 Edit Filter（编辑过滤器）页面并修改过滤器属性。

删除过滤器

将过滤器从 Filters（过滤器）列表删除，方法是勾选过滤器名称左侧的复选框并单击 **Delete（删除）**。只能删除未被策略使用的过滤器。

创建和配置过滤器

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

要创建新过滤器，请在 **Main（主页）> Policy Management（策略管理）> Filters（过滤器）**页面上单击 **Add（添加）**。输入过滤器的名称和说明，然后选择要使用的过滤器类型。选择的过滤器类型决定了可配置的过滤器设置。从以下类型中选择:

- *自定义内容*（第 112 页）
- *URL 扫描*（第 115 页）
- *Websense 防病毒*（第 116 页）
- *Websense Antispam*（第 117 页）
- *商业群发电子邮件*（第 118 页）
- *Websense ThreatScope*（第 118 页）
- *免责声明*（第 120 页）

自定义内容

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用自定义内容过滤器允许 Email Security 根据您配置的条件扫描邮件。在 **Main（主页）> Policy Management（策略管理）> Filters（过滤器）> Add Filter（添加过滤器）**（或 **Edit Filter（编辑过滤器）**）页面上，添加或修改自定义内容过滤器。Email Security 不提供默认的自定义内容过滤器。

通过在 Filter Properties（过滤器属性）区域选择下列选项之一，可以选择在匹配单个条件或匹配所有已定义条件时触发过滤器:

- **Match all conditions（匹配所有条件）**
- **Match any condition（匹配任意条件）**

通过单击 Filter Conditions（过滤器条件）框中的 **Add（添加）**，从选择的标准指定自定义过滤器的条件，包括邮件属性和操作符。在 Add Condition（添加条件）对话框中，选择下列邮件属性和操作符来配置自定义过滤器（除 DKIM 验证以外，所有邮件属性都包含用户可配置的 **Filtering criteria（过滤器标准）**输入字段）：

邮件属性	操作符选项	其他选项
Sender IP address（发件人 IP 地址）	Is（是）、Is not（不是）	None（无）
Envelope sender（信封发件人）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	None（无）
Envelope recipient（信封收件人）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	None（无）
Number of envelope recipients（信封收件人数量）	Equals（等于）、Does not equal（不等于）、Is less than（小于）、Is greater than（大于）	None（无）
From field address（发件人字段地址）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	None（无）
To field address（收件人字段地址）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	None（无）
Cc field address（抄送字段地址）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	None（无）

邮件属性	操作符选项	其他选项
Message subject（邮件主题）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	Match case（匹配大小写）
Message header: partial（邮件头：部分）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	邮件属性文本（用户配置）、Match case（匹配大小写）
Message header: complete（邮件头：完整）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	Match case（匹配大小写）
Message body text（邮件正文）	Contains（包含）、Does not contain（不包含）、Matches regular expression（匹配正则表达式）、Does not match regular expression（不匹配正则表达式）	Match case（匹配大小写）
Message size（邮件大小）	Equals（等于）、Does not equal（不等于）、Is less than（小于）、Is greater than（大于）	Filtering criteria is in KB（过滤标准以 KB 为单位）
DKIM verification result（DKIM 验证结果）	DKIM verification is successful（DKIM 验证成功）、DKIM verification failed（DKIM 验证失败）	None（无）
True Source IP（真实源 IP）	Is（是）、Is not（不是）	None（无）
Digital Fingerprinting analysis result（数字指纹分析结果）	Is spam（是垃圾邮件）、Is clean（清洁）	None（无）
LexiRules analysis result（LexiRules 分析结果）	Is spam（是垃圾邮件）、Is clean（清洁）	None（无）

邮件属性	操作符选项	其他选项
Heuristics analysis result（启发式分析结果）	Equals（等于）、Is less than（小于）、Is greater than（大于）	输入从 0 - 25 的浮点值。例如，值 6 对应启发式分析的“中”级。
Hybrid service analysis result（混合服务分析结果）（仅当您的订购包含 Email Security Gateway Anywhere 时才可用）	Equals（等于）、Is less than（小于）、Is greater than（大于）	输入从 0 - 25 的浮点值。例如，混合服务使用阈值 6 将邮件指定为垃圾邮件。

通过勾选 Filter Conditions（过滤器条件）列表中过滤器旁边的复选框并单击 **Move Up（上移）**或 **Move Down（下移）**，可以更改过滤器条件的顺序。

将一组过滤器条件从列表中删除，方法是勾选过滤器旁边的复选框并单击 **Remove（删除）**。

> **注**
> 可使用 Add Rule（添加规则）或 Edit Rule（编辑规则）页面为自定义内容过滤器添加规则。在尝试添加自定义内容规则之前，必须已经定义自定义内容过滤器。有关信息，请参阅添加规则（第 130 页）。

URL 扫描

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

URL 扫描分析电子邮件内容中的嵌入式 URL，并根据已知垃圾邮件 URL Websense 数据库将其归类。在 **Main（主页）> Policy Management（策略管理）> Filters（过滤器）> Add Filter（添加过滤器）**（或 **Edit Filter（编辑过滤器）**）页面上选择 URL 扫描过滤器类型时，勾选 **URL scanning（URL 扫描）**复选框，在 Filter Properties（过滤器属性）区域显示 URL 类别列表。选择想要 Email Security 检测的 URL 类别。当过滤器在邮件中检测到选定类别的 URL 时，就会应用任何已配置的过滤器响应。

该过滤器仅在系统包含 Websense Web Security 并已配置下载服务器时可用。有关与 Web Security 集成以使用该过滤器的详细信息，请参阅使用 *Web Security* 的 *URL* 扫描（第 43 页）。

> **注**
> 提供过滤器操作选项“Resume message scanning（恢复邮件扫描）”，以便在检测到 URL 匹配后继续运行邮件扫描。有关信息，请参阅创建和配置过滤器操作（第 122 页）。

通过勾选相应的复选框，在 **URL Categories（URL 类别）**列表中选择想要过滤器扫描的 URL 类别。勾选 **All（所有）**复选框将选中列表中的全部 URL 类别。

配置下列任意过滤器响应:

- **Replace matching URLs with（将匹配 URL 替换为）**。勾选该复选框将启用过滤器，使用文本字符串替换邮件中属于目标类别的 URL。在复选框右侧的输入字段中输入替换文本（最大长度为 128 个字符）。

  注
  在邮件分析中检测到匹配 URL 时，URL 过滤器不会扫描邮件其余的内容，也可能不会替换后续 URL。例如，如果在邮件标题中检测到 URL，则不会分析邮件正文，也不会检测邮件正文中的 URL 并予以替换。

- **Bypass URL scanning if message size exceeds（若邮件大小超出时绕过 URL 扫描）**。如果想要使用邮件大小来确定是否绕过 URL 扫描，请勾选该复选框并输入以 KB 为单位的邮件大小（默认值为 128）。

仪表盘图表总结了 Email Security 检测到的嵌入式 URL 实例。有关这些图表的名称，请参阅可用仪表盘图表（第 14 页）。

Websense 防病毒

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

防病毒扫描可检查电子邮件及任何附件是否存在电子邮件附带的病毒和威胁。

通过以下 **Filter scanning（过滤器扫描）**选项配置过滤器扫描邮件病毒的方式:

- **Treat errors as infected（将错误视为已受感染）**。如果防病毒扫描遇到错误，则会将电子邮件视为已受感染。默认设置为打开。
- **Treat encrypted files as infected（将加密文件视为已受感染）**。以防病毒引擎所不理解的方式进行加密的邮件会被视为已受感染。默认设置为打开。
- **Treat suspicious document as infected（将可疑文档视为已受感染）**。如果防病毒扫描遇到包含活动内容（包括漏洞和恶意脚本）的 PDF 文档，邮件将被视为已受感染。默认设置为关闭。
- **Treat malicious embedded iFrame as infected（将恶意嵌入的 iFrame 视为已受感染）**。如果防病毒扫描检测到包含隐藏的恶意 iFrame 的 HTML 页面，邮件将被视为已受感染。默认设置为关闭。
- **Scan message body for viruses（扫描邮件正文是否存在病毒）**。将扫描邮件内容是否存在无法正常扫描的嵌入式恶意脚本。如果邮件格式问题导致附件被视为消息正文的一部分，则将会扫描附件并检测病毒。默认设置为关闭。

配置您要在 **Heuristic level（启发级别）**部分执行的 4 种启发式分析级别的其中 1 种，顺序是从限制性最低（启发式分析已禁用）到限制性最高。默认设置为 **Enable normal level of heuristics（启用正常启发级别）**。

配置下列过滤器响应之一:

- **Remove infected attachments（删除受感染附件）**。删除触发防病毒过滤器的附件。
- **Take no action（不采取任何操作）**。这是默认操作。附件和病毒存储在预定义的位置（有关信息，请参阅创建和配置过滤器操作（第 122 页））。如果需要，可将邮件发送至管理员，告知邮件中发现了病毒。

您也可以给怀疑存在病毒的电子邮件添加通知，以提醒收件人邮件可能已受感染。使用 **Advanced（高级）**设置来配置通知功能:

1. 勾选 **Notify recipient（通知收件人）**复选框以启用通知功能。
2. 在复选框下面的输入字段中输入所需的通知文本（最长 8192 个字符，每行最多 990 个字符，换行符占 2 个字符）。
3. 指定通知应出现于邮件的顶部还是底部。默认位置为邮件的顶部。

Websense Antispam

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

防垃圾邮件扫描功能可检查电子邮件是否存在各种垃圾邮件特征。如果 Email Security Gateway Anywhere 环境中已启用混合服务并将其配置为预过滤器，则它会执行防垃圾邮件扫描。如果混合服务未配置或不可用，则 Email Security Gateway 将使用一系列其他工具进行有效的防垃圾邮件扫描。

混合服务会分析入站电子邮件并阻止其识别为垃圾邮件的任何邮件。混合服务允许进入系统进行处理的邮件包含带有扫描结果分数的标题。Email Security 使用此分数来决定邮件的处理方式。如果该分数超出垃圾邮件阈值，Email Security 会将邮件视为垃圾邮件并根据适用的策略对其进行处理。在这种情况下，Email Security Gateway 不会独自执行防垃圾邮件扫描。

混合服务必须已配置并正在运行，此选项才会显示。在 **Hybrid Service Analysis（混合服务分析）**框中，勾选 **Use email hybrid service analysis with a threshold score for spam of（对垃圾邮件使用电子邮件混合服务分析加阈值分数）**复选框，以启用混合服务垃圾邮件评分。从下拉列表中选择垃圾邮件分数（浮点值介于 0 和 20 之间，默认值为 6）。

如果此复选框未勾选（默认状态）或混合服务未启用，则 Email Security Gateway 会使用 Filter Properties Tools（过滤器属性工具）列表中的任意一种工具或所有工具执行完整的防垃圾邮件扫描。

- **Digital Fingerprinting scanning（数字指纹扫描）**。当此选项已启用时，数字指纹扫描会检查内容是否包含已知垃圾邮件的任何数字指纹。
- **LexiRules scanning（LexiRules 扫描）**。当此选项已启用时，LexiRules 扫描会分析电子邮件内容是否存在垃圾邮件常见的字模式。
- **Heuristics scanning（启发式扫描）**。当此选项已启用时，启发式扫描会检查邮件头或内容是否存在垃圾邮件特征。

  设置启发式扫描敏感度级别，从最低到最高（默认设置为 Medium（中））。

如果您想让邮件大小决定是否绕过防垃圾邮件扫描，请勾选 **Bypass antispam scanning if message size exceeds（邮件大小超出时绕过防垃圾邮件扫描）**复选框，然后输入以 KB 为单位的邮件大小（默认大小为 1024）。

商业群发电子邮件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

与垃圾邮件不同，商业群发电子邮件通常是由收件人自己索取的，有时是无意之举。例如，用户也许不注意清除“退出型”隐私权表格上的“与选定的合作伙伴分享我的个人信息”复选框。商业群发电子邮件过滤器可以对邮件进行分析，确定该邮件是由第三方群发电子邮件管理公司发出，还是直接由企业发出。

如果您的订购包含电子邮件混合服务，则可以激活商业群发电子邮件分析，将其作为混合服务预过滤流程的一部分。预过滤的结果会添加到邮件标题中，传送给本地 Email Security，由其使用混合服务评分来确定如何处理邮件。勾选 **Use hybrid service scanning result to determine the type of on-premises scanning to perform（使用混合服务扫描结果确定要执行的本地扫描类型）**选项，以启用该功能。

选择商业群发电子邮件过滤器类型后，请选择过滤器的敏感度级别:

- **Normal: Analyze email source.（标准：分析电子邮件来源。）**如果您希望过滤器仅检测来自间接（第三方）群发电子邮件来源的电子邮件，请使用此选项（默认）。
- **High: Analyze email source and content.（高：分析电子邮件来源和内容。）**如果您希望过滤器对直接和间接来源的群发电子邮件都加以检测，请使用此选项。

如果您想让邮件大小决定是否绕过商业群发电子邮件分析，请勾选 **Bypass commercial bulk email detection if message size exceeds（邮件大小超出时绕过商业群发电子邮件检测）**复选框，然后输入以 KB 为单位的邮件大小（默认大小为 1024）。

可以对该过滤器进行设置，使用商业群发电子邮件默认过滤器操作。有关信息，请参阅管理过滤器操作（第 121 页）。

Websense ThreatScope

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Websense ThreatScope 包括文件沙盒功能，是一款云托管沙盒，用于对常见威胁的文件类型进行深度内容检测（包括 .exe、.pdf、.xls、.xlsx、.doc、.docx、.ppt、.pptx，以及存档文件）。使用 ThreatScope 过滤器为网络配置文件沙盒。仅当您的订购包含 Websense ThreatScope 时，该功能才可用。

该过滤器在监控或执行模式下均可以使用。当启用执行模式、触发过滤器，并将附件发送给文件沙盒进行分析时，还可以使用发送通知邮件的选项。您可以定义条件。当满足条件时，允许邮件绕过 ThreatScope 过滤器。

选择 ThreatScope 过滤器类型并输入名称和说明后，为过滤器指定以下其中一种操作模式:

- **Monitor（监控）**（默认）。邮件传送给其收件人，并将副本发送到文件沙盒进行分析。如果分析确定附件是清洁的，则不返回报表。如果分析确定附件是恶意的，则不将邮件复制到指定队列。可以发送有关分析结果的通知电子邮件。

  应配置相应的过滤器操作，以确保丢弃触发过滤器的电子邮件并将其保存到特定队列（**Main（主页）> Policy Management（策略管理）> Actions（操作）**）。默认队列是病毒队列。

- **Enforce（执行）**。邮件保存在队列中，直到执行文件沙盒分析。如果分析确定附件是清洁的，则恢复邮件处理。如果分析确定附件是恶意的，则隔离电子邮件。可以发送有关分析结果的通知电子邮件。

  应配置相应的过滤器操作，以确保丢弃触发过滤器的电子邮件并将其保存到特定队列（**Main（主页）> Policy Management（策略管理）> Actions（操作）**）。默认队列是病毒队列。

- **Enforce and notify（执行和通知）**。邮件保存在队列中，直到执行文件沙盒分析，并可以发送有关通知收件人分析正在进行中的电子邮件。勾选 **Send enforcement notification（发送执行通知）**复选框配置此邮件，其中包含作为附件的原始邮件。邮件附件按如下方式处理:
  - 某些文件类型转换为纯文本（.pdf、.doc/.docx、.xls/.xlsx 和 .ppt/.pptx）。
  - 其他类型的文件将被删除，只有文件名会出现在邮件中（.exe 和归档文件）。

  应配置相应的过滤器操作，以确保丢弃触发过滤器的电子邮件并将其保存到特定队列（**Main（主页）> Policy Management（策略管理）> Actions（操作）**）。默认队列是病毒队列。

电子邮件通知包含以下组成部分:

- **Sender（发件人）**。从以下选项中识别通知邮件发件人:
  - Original email sender（原始电子邮件发件人）
  - Administrator（管理员）（默认）。如果使用此选项，您必须在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面中配置有效的管理员电子邮件地址（请参阅设置系统通知电子邮件地址（第 50 页））。
  - Custom（自定义）。如果选择此选项，您仅能指定 1 个发件人地址。
- **Recipient（收件人）**。从以下选项中识别通知邮件收件人:
  - Original email recipient（原始电子邮件收件人）
  - Administrator（管理员）。如果使用此选项，您必须在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面中配置有效的管理员电子邮件地址（请参阅设置系统通知电子邮件地址（第 50 页））。
  - Custom（自定义）。如果选择此选项，您可以指定一个或多个收件人地址，地址用分号隔开。

- **Subject（主题）**。输入您要在收到通知时显示的主题。
- **Content（内容）**。输入您要在通知邮件正文中显示的文本。
- **Attachment（附件）**。指定您是否要将原始邮件包含为通知邮件的附件。从以下选项中选择一个选项:
  - Do not attach message（不附加邮件）（默认）
  - Attach filtered message（附加已过滤邮件）

有关为 ThreatScope 过滤器配置操作的信息，请参阅创建和配置过滤器操作（第 122 页）。

勾选适当的复选框，选择您希望文件沙盒查找和分析的文件类型。

可以为您希望跳过文件沙盒分析的邮件配置绕过选项。在绕过条件部分单击 **Add（添加）**并指定以下信息:

- **Condition name（条件名称）**。为每组绕过条件指定一个名称。
- **Sender email address/domain（发件人电子邮件地址 / 域名）**。输入个人的电子邮件地址或域名。使用星号 (*) 来表示通配符条目，并使用英文分号 (;) 分隔多个条目。
- **Attachment filename keyword（附件文件名关键字）**。输入含在附件文件名中的字符串。

在绕过条件表格中单击条件名称，可编辑现有的绕过条件组。

如果您想根据邮件大小决定是否绕过文件沙盒分析，请勾选 **Bypass ThreatScope analysis if message size exceeds（邮件大小超出时绕过 ThreatScope 分析）**复选框，然后输入目标文件大小（默认为 32 MB）。

要了解进一步的信息，请参阅 ThreatScope 产品文档和 Websense 隐私权政策 (www.Websense.com)。

免责声明

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

免责声明过滤器会自动将已定义的文本添加到邮件的开头或结尾。在 Add Filter（添加过滤器）或 Edit Filter（编辑过滤器）页面的 Filter Properties（过滤器属性）部分为 Disclaimer（免责声明）过滤器指定所需的文本。

可以用任何语言来撰写主免责声明，只要电子邮件支持该字符集。

次免责声明必须用英语撰写，以便在电子邮件不支持主免责声明字符集时使用。

免责声明文本的长度可以介于 4 到 8192 个字符之间。换行符占 2 个字符。

指定免责声明应在电子邮件中出现的位置:

- **Beginning of message（邮件开头）**
- **End of message（邮件结尾）**

勾选 **Enable Report Spam feature（启用报告垃圾邮件功能）**复选框可允许邮件收件人将其报告为垃圾邮件。通过免责声明文本中的链接，收件人可进入 Personal Email Manager，在此处可将邮件从隔离邮件列表中作为垃圾邮件报告给 Websense。

管理过滤器操作

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

过滤器操作决定邮件的最终处理。Email Security Gateway 会分析邮件及其附件，然后根据适用的策略设置执行操作。操作在 **Main（主页）> Policy Management（策略管理）> Actions（操作）**页面创建。配置电子邮件策略时，您可以将已定义的操作添加到策略规则。

除了定义 Email Security Gateway 策略中使用的操作外，您还可以创建用于 Data Security 中电子邮件 DLP 操作计划的操作。对于大多数网络配置（即单个独立设备或单个设备集群）来说，可用于为电子邮件 DLP 策略创建操作的属性设置与 Email Security Gateway 策略操作的属性设置相同。但是，如果您的网络中包含多个独立设备或多个集群，在创建操作时可用的 DLP 策略操作设置会受到限制。除非另有说明，否则以下步骤同时适用于 Email Security 和 Data Security 策略操作。

创建新的过滤器操作，方法是单击 **Add（添加）**并选择操作属性（请参阅创建和配置过滤器操作（第 122 页））。

您可以删除现有过滤器，方法是勾选过滤器名称左侧的复选框以将其选定并单击 **Delete（删除）**。仅当过滤器操作的当前状态为 **Not referenced（未引用）**（即该操作当前未在策略规则中使用）时，您才可以删除它。当前为某个过滤器所引用的过滤器操作没有可供选择的复选框。您不能删除 Email Security 的默认过滤器操作。

Email Security 提供以下默认操作:

- **Virus（病毒）**。丢弃已过滤的邮件并将原始邮件保存到病毒队列。允许 Personal Email Manager 最终用户查看和管理邮件。
- **URL Scanning（URL 扫描）**。丢弃已过滤的邮件并将原始邮件保存到垃圾邮件队列。允许 Personal Email Manager 最终用户查看和管理邮件。
- **Spam（垃圾邮件）**。丢弃已过滤的邮件并将原始邮件保存到垃圾邮件队列。允许 Personal Email Manager 最终用户查看和管理邮件。
- **Commercial Bulk（商业群发电子邮件）**。传送已过滤的邮件并将“COMMERCIAL:”添加到邮件主题中。允许 Personal Email Manager 最终用户查看和管理邮件。
- **ThreatScope**。丢弃已过滤的邮件并将原始邮件保存到病毒队列。发送通知邮件，不会将原始电子邮件附加给原始电子邮件发件人。

创建和配置过滤器操作

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以在 **Main（主页）> Policy Management（策略管理）> Actions（操作）** 页面上添加过滤器操作并配置其属性。单击 **Add（添加）**，以打开 Add Action（添加操作）页面并输入操作名称。

在 **Used by（使用者）**下拉列表中，选择此操作可用于的策略类型：**Email Security** 或 **Data Security**。您在此处的选择决定了在创建操作时可使用哪些操作属性。

Email Security Gateway 策略操作选项包括:

- Deliver message（传送邮件）（默认）
- Resume Processing（恢复处理）
- Drop message（丢弃邮件）

Data Security 策略操作选项包括:

- Resume processing（恢复处理）（默认）
- Drop message（丢弃邮件）

传送邮件和恢复处理选项包括相同的操作属性。但是，其针对单个设备 / 集群网络中 Email Security 策略操作和 Data Security 策略操作的行为不同于其针对在多个设备 / 集群环境中创建的 Data Security 策略操作的行为。

传送邮件

当您希望 Email Security Gateway 将电子邮件传送给其预期收件人时，选择 **Deliver message（传送邮件）**。此选项是 Email Security 策略操作的默认选择，且不适用于 Data Security 策略操作。

如果选择此选项，您还可以定义以下邮件传送选项:

- **Enable header modification（启用标题修改）**。勾选此复选框可打开一组标题修改条件输入字段。包括以下选项:

条件	参数
Add or rewrite header value（添加或改写标题值）	Header name（标题名称）、To value（收件人值）
Remove header（删除标题）	Header name（标题名称）
Remove header if condition matches（如果条件匹配则删除标题）	Header name（标题名称）、If header contains the value（如果标题包含值）
Find and replace header value（查找和替换标题值）	Header name（标题名称）、Find（查找）、Replace with（替换为）

条件	参数
Add or append to header value（添加或在后面附加标题值）	Header name（标题名称）、Add/append value（添加 / 在后面附加值）
Add or prepend to header value（添加或在前面附加标题值）	Header name（标题名称）、Add/prepend value（添加 / 在前面附加值）

单击每个条件行末尾的图标，可以删除当前的标题修改条件，或在当前条件下方添加新条件。

- **Bcc the original unfiltered message to（将原始的未过滤邮件密送至）**。输入至少 1 个您想将未过滤邮件的无信头副本发送到的电子邮件地址，例如电子邮件系统管理员。使用英文分号分隔多个电子邮件地址。
- **Delay message delivery until（延迟邮件传送直到）**。指定延迟邮件传送的日期和时间。如果由于某种原因想要延迟邮件的传送，则可以选择该选项。建议该操作选项与策略规则中的自定义内容过滤器一起使用。有关自定义内容过滤器的信息，请参阅自定义内容（第 112 页）。
- **Use IP address（使用 IP 地址）**。从邮件传送下拉列表中指定一个设备 IP 地址。如果您希望路由大量出站电子邮件，该功能非常有用。建议该操作选项与策略规则中的自定义内容过滤器一起使用。有关自定义内容过滤器的信息，请参阅自定义内容（第 112 页）。

  列表中的 IP 地址在 Websense V-Series™（V 系列）设备管理器中配置。（有关信息，请参阅 Websense Appliance Manager 帮助中标题为 *Email Security virtual interfaces*（*Email Security* 虚拟接口）的主题。）
- **根据基于域的路由传送电子邮件**。指定通过定义的基于域的路由传送邮件。从下拉列表中选择所需的路由。也可以单击 **Edit Route（编辑路由）**，修改所选择的路由。
- **Save the original message to a queue（将原始邮件保存到队列）**。将邮件发送到指定邮件队列进行进一步处理。选择 **Add Queue（添加队列）**选项，为此过滤器操作添加一个新队列。
- **Personal Email Manager portal options（Personal Email Manager 门户选项）**。仅当勾选 **Save the original message to a queue（将原始邮件保存到队列）**选项时，才会启用该选项。选择以下其中一种方式，指定在 Personal Email Manager 最终用户工具中如何处理队列中的邮件:
  - **View and manage message（查看并管理邮件）**。允许最终用户查看邮件并执行 Personal Email Manager 最终用户工具中可用的任何操作。
  - **Do not show（不显示）**。确保邮件不会出现在 Personal Email Manager 最终用户门户中。
  - **Message log only（仅邮件日志）**。邮件的相关信息会出现在 Personal Email Manager 最终用户门户中，但最终用户只有有限的访问权限。用户不能查看邮件内容，不能传送、下载或转发邮件，也不能将地址添加到个人的“始终阻止”或“始终允许”列表。

恢复处理

如果您希望 Email Security Gateway 在触发当前过滤器时（例如，在邮件中检测到 URL 匹配后）继续按顺序使用下一个过滤器扫描邮件，请选择 **Resume processing（恢复处理）**。如果该选项是最后触发的过滤器操作，则传送该邮件。

此选项是 Data Security 策略操作的默认选择。

如果您正在创建 Email Security 操作或 Data Security 操作，且在单个设备 / 设备集群中配置网络，则 **Resume processing（恢复处理）**的邮件操作选项与上述 **Deliver message（传送邮件）**的相应选项相同。

但是，如果您正在创建用于 Data Security 的操作，且网络中包含多个独立设备或设备集群，则应注意以下操作属性行为差异:

- **Use IP address（使用 IP 地址）**。此选项可供选择，但是唯一支持创建 Data Security 操作的值是设备 E1 接口的 IP 地址。

  您可通过执行 **Edit Action（编辑操作）**操作更改此值。
- **根据基于域的路由传送电子邮件**。此选项可供选择，但是唯一支持创建 Data Security 操作的值是默认的域路由（**Settings（设置）> Inbound/Outbound（入站 / 出站）> Mail Routing（邮件路由）**）。

  您可通过执行 **Edit Action（编辑操作）**操作更改此值。**Edit Route（编辑路由）**选项不可用。
- **Save the original message to a queue（将原始邮件保存到队列）**。此选项可供选择，但是唯一支持创建 Data Security 操作的队列是 Email Security Gateway 默认队列。您不可以指定用户配置的队列。

  您可通过执行 **Edit Action（编辑操作）**操作更改此值。

丢弃邮件

当您希望 Email Security Gateway 在未将邮件传送给其预期收件人的情况下将邮件删除时，选择 **Drop message（丢弃邮件）**。此选项可同时用于 Email Security 和 Data Security 策略操作。

您可以勾选 **Forward to（转发至）**选项并输入至少一个电子邮件地址，转发丢弃的邮件。

也可以配置 **Save the original message to a queue（将原始邮件保存到队列）**选项，将邮件发送到指定邮件队列进行进一步处理。勾选该复选框会启用 **Personal Email Manager portal options（Personal Email Manager 门户选项）**，该选项用于确定邮件传送过滤器操作。

> **注**
> 对于在多个设备 / 集群环境中创建的 Data Security 操作，仅 Email Security Gateway 默认队列可供选择。

移除附件

如果您希望 Email Security Gateway 从电子邮件中删除附件作为策略操作的一部分，请选择 **Strip attachment（移除附件）**。此选项仅适用于 Data Security 策略操作。

发送通知

Send notification（发送通知）选项可用于配置向指定收件人发送的电子邮件的相关预定义通知。通知包含以下组成部分:

- **Sender（发件人）**。从以下选项中识别通知邮件发件人:
  - Original email sender（原始电子邮件发件人）
  - Administrator（管理员）（默认）。如果使用此选项，您必须在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面中配置有效的管理员电子邮件地址（请参阅设置系统通知电子邮件地址（第 50 页））。
  - Custom（自定义）。如果选择此选项，您仅能指定 1 个发件人地址。
- **Recipient（收件人）**。从以下选项中识别通知邮件收件人:
  - Original email sender（原始电子邮件发件人）
  - Original email recipient（原始电子邮件收件人）
  - Administrator（管理员）。如果使用此选项，您必须在 **Settings（设置）> General（一般）> System Settings（系统设置）**页面中配置有效的管理员电子邮件地址（请参阅设置系统通知电子邮件地址（第 50 页））。
  - Custom（自定义）。如果选择此选项，您可以指定一个或多个收件人地址，地址用分号隔开。
- **Subject（主题）**。输入您要在收到通知时显示的主题。默认主题为“WARNING: Message may contain malicious content.”（警告：邮件可能包含恶意内容。）
- **Content（内容）**。输入您要在通知邮件正文中显示的文本。
- **Attachment（附件）**。指定您是否要将原始邮件包含为通知邮件的附件。从以下选项中选择一个选项:
  - Do not attach message（不附加邮件）（默认）
  - Attach original unfiltered message（附加原始的未过滤邮件）
  - Attach filtered message（附加已过滤邮件）

编辑现有过滤器操作

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以编辑现有过滤器操作，方法是在 **Main（主页）> Policy Management（策略管理）> Actions（操作）**页面上单击操作名称。Edit Action（编辑操作）页面将会打开，显示当前的操作属性。修改创建和配置过滤器操作（第 122 页）中列出的任意选项。

还可以使用此操作更改在创建 Data Security 操作时配置的任何默认属性。有关默认设置的详细信息，请参阅恢复处理（第 124 页）。

管理策略

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Email Security Gateway 策略根据已定义的发件人 / 收件人条件和电子邮件的定向进行应用。您可以将不同的策略应用到不同的发件人群组和收件人群组。例如，您可以将一个策略应用到企业中的市场部群组，然后将另一个策略应用到人力资源群组。在一个策略中定义一组发件人和收件人之后，您可以添加策略规则，以便在电子邮件的发件人 / 收件人条件与该策略匹配时应用。

策略规则包括过滤器和过滤器操作，过滤器操作决定了符合策略的发件人 / 收件人条件的邮件的处理方式。过滤器为电子邮件分析提供了基础，过滤器操作则决定了触发某个特定过滤器时对邮件所作的最终处理。创建并配置过滤器和过滤器操作之后，您可以将它们加入到策略中。有关配置过滤器和过滤器操作的信息，请参阅管理过滤器（第 111 页）和管理过滤器操作（第 121 页）。

Email Security 包含 3 种常用策略，这取决于电子邮件的方向（入站、出站或内部）。邮件方向根据组织受保护域确定:

- 入站 — 发件人地址不来自受保护域，收件人地址处于受保护域中
- 出站 — 发件人地址来自受保护域，收件人地址不处于受保护域中
- 内部 — 发件人和收件人地址均处于受保护域中。

Email Security Gateway 为每个电子邮件定向提供了 1 个预定义的默认策略，并且为每个定向提供了一个默认 Data Security 策略。

Data Security 策略可能适用于任何种定向的电子邮件。这些策略在 TRITON Unified Security Center 的 Data Security 模块中进行配置，并且只能在 Email Security Gateway 中启用或禁用。您需要通过 Data Security 管理器注册 Email Security，并在 Data Security 模块中单击 **Deploy（部署）**，这样才能激活策略。有关详细信息，请参阅启用 *Data Security* 策略（第 127 页）。

更改策略顺序

添加策略之后，您可以选择该策略并使用 **Move Up（上移）**和 **Move Down（下移）**按钮在策略列表中将其上下移动，以便指定应用该策略的条件。当邮件条件与一个策略匹配时，将不应用列表中的后续策略。

您不能更改默认策略的顺序。它们在邮件没有匹配其它任何策略时最后应用。

删除策略

您可以删除策略，方法是在 Policies（策略）页面上勾选策略名称旁边的复选框，然后单击 **Delete（删除）**。请注意，您不能删除默认策略。

相关主题:

- 启用 *Data Security* 策略（第 127 页）
- 创建策略（第 128 页）
- 添加发件人 / 收件人条件（第 129 页）
- 添加规则（第 130 页）
- 编辑规则（第 131 页）

启用 Data Security 策略

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

除了创建和启用可保护您的电子邮件系统免受病毒和垃圾邮件侵害的策略之外，您还可以启用可检测组织电子邮件中是否存在敏感性数据并执行适当操作以防止数据丢失的 Websense Data Security 策略。您可以将 Data Security 策略用于入站、出站和内部电子邮件。

Data Security 电子邮件 DLP 策略必须在 Websense Data Security 模块（**Main（主页）> Policy Management（策略管理）> DLP Policies（DLP 策略）> Manage Policies（管理策略）**）中配置。一个新的策略向导提供了创建新的 Data Security 电子邮件 DLP 策略的相关步骤。有关详细信息，请参阅 *Data Security 管理器帮助*。

如果您希望使用邮件加密，则应在 Data Security 中创建数据泄露防护策略。确保策略具有“加密”操作计划。有关 Email Security Gateway 加密选项的信息，请参阅处理加密的邮件（第 105 页）。

还可以在 Email Security Gateway 中创建过滤器操作以用于 Data Security 操作计划。有关配置 Data Security 过滤器操作的信息，请参阅创建和配置过滤器操作（第 122 页）。

Data Security 策略在 Email Security Gateway 中默认为启用。但是，您必须通过 Data Security 管理器注册 Email Security，策略才能应用到电子邮件。有关如何注册 Data Security 的说明，请参阅向 *Websense Data Security* 注册（第 41 页）。

如果您由于某种原因而需要在 Email Security Gateway 中启用 Data Security 策略，请在入站、出站或内部电子邮件的 **Main（主页）> Policy Management（策略管理）> Policies（策略）**页面上单击 Data Security 策略名称，然后在 Edit Policy（编辑策略）页面中设置以下选项:

- **Status（状态）：** 启用或禁用。在 Email Security 中启用或禁用 Data Security 策略。Data Security 策略默认启用。
- **Mode（模式）：** 监视或实施。如果您只想让 Data Security 监视电子邮件，请选择 **Monitor（监视）**；如果您想让 Data Security 将其策略应用到您的电子邮件，则选择 **Enforce（实施）**。

- **Notification（通知）**。当邮件的电子邮件附件由于 Data Security 策略而被丢弃时，给邮件添加通知。
  1. 勾选 **Send notification when attachment of the message is dropped（邮件的附件被丢弃时发送通知）**复选框，以便发送通知。
  2. 输入通知邮件文本。
  3. 确定通知文本出现在附件被丢弃的邮件的正文之上还是之下。

> **注**
> 触发了 Data Security 策略（其操作为“隔离”）的邮件将在 Data Security 隔离队列中隔离，而不是在 Email Security Gateway 队列中隔离。邮件可由 Data Security 释放以进行传送。

创建策略

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用 **Main（主页）> Policy Management（策略管理）> Policies（策略）**页面来创建新的入站、出站或内部策略。

1. 单击 **Add（添加）**，以打开 Add Policy（添加策略）页面并输入唯一的 **Policy name（策略名称）**。策略名称必须介于 4 到 50 个字符之间。不建议在策略名称中使用以下特殊字符:

   * < > { } ~ ! $ % & @ # . " | \ & + = ? / ; : ,

   策略名称可以包含空格、破折号和省略号。
2. 为策略输入清楚而简洁的 **Description（说明）**。

   适用于策略名称的特殊字符建议也适用于说明。
3. 在 **Order（顺序）**字段中定义此策略的应用顺序。

   默认情况下，新的策略置于列表顶部。您不能给多个策略应用相同的序号。如果您选择一个已被使用的编号，则当前使用该编号的策略以及该策略之下的所有策略在列表中都将下移 1 位。
4. 定义 **Sender/Recipient Conditions（发件人 / 收件人条件）**。

   默认情况下，每个新策略都包含一个发件人 / 收件人条件，该条件将策略应用到所有电子邮件发件人和收件人。要添加更多条件，请单击 **Add（添加）**，然后参阅添加发件人 / 收件人条件（第 129 页）。

> **注**
> 您必须定义至少 1 个发件人 / 收件人条件。如果策略不包含任何发件人 / 收件人条件，该策略将不会被应用。

5. 编辑可用的 **Rules（规则）**，以便根据此策略调整过滤器和操作。单击规则名称，然后参阅编辑规则（第 131 页）。
6. 单击 **OK（确定）**以保存策略。

添加发件人 / 收件人条件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用 **Add Policy（添加策略）> Add Sender/Recipient Condition（添加发件人 / 收件人条件）**页面来指定此策略将应用到的发件人和收件人。您可以根据需要来设置策略的应用范围，例如应用到所有用户或收到来自某个特定域的邮件的所有用户，或者仅应用到特定的电子邮件地址。

对于每个发件人 / 收件人条件，您必须选择一个 **Sender Source（发件人源）**和 **Recipient Source（收件人源）**：

- 如果您选择 **Local Address（本地地址）**，请输入发件人或收件人电子邮件地址以与策略配合使用。您可以使用星号通配符来指定组合，例如:
  - *.mycompany.com 会将策略应用到具有 mycompany.com 电子邮件地址的所有用户
  - *sales@mycompany.com 会将策略应用到 mycompany.com 中所有电子邮件地址的子集，例如 us_sales@mycompany.com 和 uk_sales@mycompany.com
  - john.doe@mycompany.com 会将策略应用到某个特定用户。

  要将策略应用到所有电子邮件地址，请输入星号 (*)。
- 如果您选择 **User directory（用户目录）**，请从下拉列表中选择目录源。您必须先设置要连接到的用户目录，然后才能选择此选项。选择 **Add User Directory（添加用户目录）**以创建新的目录源。
- 如果选择 **Domain group（域组）**，请从现有域组的下拉列表中选择来源域，或选择 **Add Domain Group（添加域组）**，添加新的域组。

选择好之后，请单击 **OK（确定）**以返回到 Add Policy（添加策略）或 Edit Policy（编辑策略）页面。

删除发件人 / 收件人条件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

要删除发件人 / 收件人条件，请在 Add Policy（添加策略）或 Edit Policy（编辑策略）页面上选中条件 ID 旁边的复选框，然后单击 **Delete（删除）**。

策略应包含至少 1 个发件人 / 收件人条件。

添加规则

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

策略规则包括过滤器和当邮件触发过滤器时采取的 Email Security 操作。过滤器将应用于匹配策略的发件人 / 收件人条件的邮件。Email Security Gateway 提供以下默认规则:

- **Antivirus（防病毒）**。启用规则，并使用默认的病毒过滤器和过滤器操作。
- **URL Scanning（URL 扫描）**。启用规则，并使用默认的 URL 扫描过滤器和过滤器操作。
- **Antispam（防垃圾邮件）**。启用规则，并使用默认的垃圾邮件过滤器和过滤器操作。
- **Commercial Bulk（商业群发）**。启用规则，并使用默认的商业群发电子邮件过滤器和过滤器操作。
- **ThreatScope**。启用规则，并使用默认的 ThreatScope 过滤器和过滤器操作。
- **Disclaimer（免责声明）**。启用规则，但当启用时，使用默认的免责声明过滤器。

只能创建与自定义内容过滤器相结合的新规则。

通过以下步骤，使用自定义内容过滤器添加策略规则:

1. 单击 Rules 部分中的 **Add（添加）**以打开 Add Rule（添加规则）页面。
2. 在 **Rule Name（规则名称）**输入字段输入规则的名称。
3. 选择所需策略状态: **Enabled（启用）**（默认设置）或 **Disabled（禁用）**。
4. 选择规则的应用顺序。默认情况下，新创建的自定义内容规则会出现在第一个位置。使用 **Move Up（上移）**和 **Move Down（下移）**按钮可调整自定义内容规则的顺序。免责声明规则始终最后应用。
5. 从 **Filter name（过滤器名称）**下拉列表中选择自定义内容过滤器。如果还没有创建自定义内容过滤器，该列表将仅包含 **Add filter（添加过滤器）**条目。选择该条目打开 Add Filter（添加过滤器）页面以定义新的自定义内容过滤器。该过滤器类型始终为 **Custom Content（自定义内容）**。有关信息，请参阅创建和配置过滤器（第 112 页）。
6. 以下列方式之一配置过滤器操作:
   - 从 **Action name（操作名称）**下拉列表中选择默认过滤器操作。如果想要更改默认操作设置，请单击 **Edit（编辑）**。
   - 也可以通过从下拉列表中选择 **Add Action（添加操作）**来创建新操作。

   有关信息，请参阅创建和配置过滤器操作（第 122 页）。

编辑规则

单击规则名称，然后使用 **Add Policy（添加策略）> Edit Rule（编辑规则）**页面来定义与发件人 / 收件人条件匹配并触发策略的电子邮件的处理方式。此页面包含当前定义您所单击的规则的过滤器和过滤器操作。也可定义邮件发件人 / 收件人条件，在符合条件时允许邮件绕过过滤器。

编辑过滤器

要编辑过滤器，请在 Filter（过滤器）部分单击 **Edit（编辑）**，以打开 Edit Filter（编辑过滤器）页面。修改过滤器特征，如创建和配置过滤器（第 112 页）中所述。

编辑过滤器操作

要编辑过滤器，请在 Action（操作）部分单击 **Edit（编辑）**，以打开 Edit Action（编辑操作）页面。修改操作选项，如创建和配置过滤器操作（第 122 页）中所述。

> **注**
> 对现有规则组件所作的任何更改将反映到您在 **Main（主页）> Filters（过滤器）**页面和 **Main（主页）> Actions（操作）**页面中配置的过滤器和操作定义。更改并非个别策略所独有的。

添加过滤器绕过条件

要添加过滤器绕过条件，请单击 Filter Bypass Condition（过滤器绕过条件）部分的 **Add（添加）**以打开 Add Filter Bypass Conditions（添加过滤器绕过条件）页面。可以下列方式之一在 Sender Email Addresses（发件人电子邮件地址）及 Recipient Email Addresses（收件人电子邮件地址）部分创建过滤器绕过条目：

- 通过单击 Email Address File（电子邮件地址文件）右侧的 **Browse（浏览）**并导航至所需的文本文件，添加预定义的电子邮件地址列表。文件格式应为每行 1 个电子邮件地址，最多可添加 8 个地址。
- 在 **Email address（电子邮件地址）**字段中输入单个电子邮件地址。单击右箭头按钮，以将单个条目添加到右侧的 **Email Address List（电子邮件地址列表）**。

星号 (*) 可作为通配符用在地址中。

单击 **OK（确定）**以保存绕过条目。

选择 Email Address List（电子邮件地址列表）中的条目并单击 **Remove（删除）**，可从列表中删除该条目。单击 **Export All（导出全部）**可将地址列表导出并保存为文本文件。

不能使用这些设置来绕过自定义内容过滤器。

编辑现有策略

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以编辑现有策略，方法是在 Policies（策略）页面上单击其名称以打开 Edit Policy（编辑策略）页面。编辑说明、状态、发件人 / 收件人条件和规则，如创建策略（第 128 页）中所述。您将不能编辑策略名称。

您只能编辑已创建策略的策略顺序，不能编辑默认策略的策略顺序。

管理全局 Always Block（始终阻止）列表和 Always Permit（始终允许）列表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

维持始终阻止或始终允许的 IP 和电子邮件地址的列表，有助于提高 Email Security Gateway 系统的效率。让受信任的邮件绕过系统垃圾邮件和病毒扫描功能可以节省带宽和时间。

注
来自全局 Always Permit（始终允许）列表中的地址的邮件将受到其他 Email Security Gateway 过滤，包括邮件控制、连接控制、帐户搜集攻击和转发控制。

管理 Always Block（始终阻止）列表

您可以直接从 **Main（主页）> Policy Management（策略管理）> Always Block/ Permit（始终阻止 / 允许）**页面将 IP 或电子邮件地址添加到 Always Block（始终阻止）列表中。您也可以添加预定义的 IP 或电子邮件地址列表，将各个条目从列表中删除，将列表作为文本文件导出到桌面，以及搜索列表。

来自同时出现在 Always Block（始终阻止）列表和 Always Permit（始终允许）列表中的电子邮件地址的邮件将被允许。来自同时出现在两个列表中的 IP 的邮件将被阻止。

完成添加地址条目之后，您可以将列表导出为文本文件，方法是单击 **Export All（导出全部）**按钮并打开文本文件或将其另存到所需的位置。

删除单个条目，方法是在 IP 电子邮件地址列表中将其选定并单击 **Remove（删除）**。您也可以在列表中搜索条目，方法是在搜索字段中输入关键字并单击 **Search（搜索）**。

将 IP 地址添加到 Always Block（始终阻止）列表

使用以下步骤将 IP 地址添加到 Always Block（始终阻止）列表:

1. 单击 **Always Block（始终阻止）**选项卡。
2. 在页面的 IP Address Block List（IP 地址阻止列表）部分，添加预定义的 IP 地址，方法是单击 **Browse（浏览）**并导航到所需的文本文件。文件格式应为每行 1 个 IP 地址，并且文件最大不得超过 10 MB。
3. 您也可以在 **IP/Subnet address（IP/ 子网地址）**字段中输入单个 IP/ 子网地址。单击右箭头按钮，以将单个条目添加到右侧的 **IP Address List（IP 地址列表）**。
4. 单击 **OK（确定）**。

将电子邮件地址添加到 Always Block（始终阻止）列表

使用以下步骤将电子邮件地址添加到 Always Block（始终阻止）列表:

1. 单击 **Always Block（始终阻止）**选项卡。
2. 在 Email Address Block List（电子邮件地址阻止列表）部分，添加预定义的电子邮件地址，方法是单击 **Browse（浏览）**并导航到所需的文本文件。文件格式应为每行 1 个电子邮件地址，并且文件最大不得超过 10 MB。
3. 您也可以在 **Email address（电子邮件地址）**字段中输入单个电子邮件地址。单击右箭头按钮，以将单个条目添加到右侧的 **Email Address List（电子邮件地址列表）**。
4. 单击 **OK（确定）**。

管理 Always Permit（始终允许）列表

您可以直接从 **Main（主页）> Policy Management（策略管理）> Always Block/ Permit（始终阻止 / 允许）**页面将 IP 或电子邮件地址添加到 Always Permit（始终允许）列表。您也可以添加预定义的 IP 或电子邮件地址列表，将各个条目从列表中删除，将列表作为文本文件导出到桌面，以及搜索列表。

来自同时出现在 Always Block（始终阻止）列表和 Always Permit（始终允许）列表中的电子邮件地址的电子邮件将被允许。来自同时出现在两个列表中的 IP 的邮件将被阻止。

完成添加地址条目之后，您可以将列表导出为文本文件，方法是单击 **Export All（导出全部）**按钮并打开文本文件或将其另存到所需的位置。

删除单个条目，方法是在 IP 电子邮件地址列表中将其选定并单击 **Remove（删除）**。您也可以在列表中搜索条目，方法是在搜索字段中输入关键字并单击 **Search（搜索）**。

将 IP 地址添加到 Always Permit（始终允许）列表

使用以下步骤将 IP 地址添加到 Always Permit（始终允许）列表:

1. 单击 **Always Permit（始终允许）**选项卡。
2. 在页面的 IP Address Permit List（IP 地址允许列表）部分，添加预定义的 IP 地址，方法是单击 **Browse（浏览）**并导航到所需的文本文件。文件格式应为每行 1 个 IP 地址，并且文件最大不得超过 10 MB。
3. 您也可以在 **IP/Subnet address（IP/ 子网地址）**字段中输入单个 IP/ 子网地址。单击右箭头按钮，以将单个条目添加到右侧的 **IP Address List（IP 地址列表）**。
4. 单击 **OK（确定）**。

将电子邮件地址添加到 Always Permit（始终允许）列表

使用以下步骤将电子邮件地址添加到 Always Permit（始终允许）列表:

1. 单击 **Always Permit（始终允许）**选项卡。
2. 在 Email Address Permit List（电子邮件地址允许列表）部分，添加预定义的电子邮件地址，方法是单击 **Browse（浏览）**并导航到所需的文本文件。文件格式应为每行 1 个电子邮件地址，并且文件最大不得超过 10 MB。
3. 您也可以在 **Email address（电子邮件地址）**字段中输入单个电子邮件地址。单击右箭头按钮，以将单个条目添加到右侧的 **Email Address List（电子邮件地址列表）**。
4. 单击 **OK（确定）**。

启用 Dynamic Always Permit List（动态始终允许列表）

启用 Dynamic Always Permit List（动态始终允许列表）功能可让发件人地址与收件人地址之间交换的部分邮件进行配对，以绕过防垃圾邮件过滤。当发件人与收件人之间的邮件不会触发防垃圾邮件过滤器达到指定次数之后，该发件人 / 收件人地址对将被添加到 Dynamic Always Permit List（动态始终允许列表）。将不会对此发件人 / 收件人地址对之间的邮件执行防垃圾邮件过滤。当指定的超时期限过去之后，地址对会从列表中删除。

Enable Dynamic Always Permit list（启用动态始终允许列表）复选框在 Dynamic Always Permit List（动态始终允许列表）部分默认为启用。您可以修改以下设置:

1. 在 **Occurrence（次数）**字段中，指定将发件人 / 收件人对添加到列表中所需的无垃圾邮件电子邮件交换次数（从 1 到 5）。默认值为 1。
2. 在 **Timeout（超时）**字段中，为超时间隔输入一个单位为小时的值（从 1 到 720）。默认值为 720。

手动清空列表，方法是单击 **Clear Dynamic Always Permit List（清空动态始终允许列表）**按钮。请注意，如果您禁用此功能，列表将自动清空。

6 使用报表

主题:

配置 Log Database 选项

Log Database 用于记录存储电子邮件流量活动，以及针对该流量执行的相关 Email Security Gateway 过滤操作。这些数据记录用于生成 Email Security 活动的演示报表，包括电子邮件的大小和信息量以及发件人和收件人的标识。还用于在仪表盘中生成状态图表。

管理 Log Database 需要控制数据库操作的多个方面，包括维护任务的定时、创建新数据库分区的条件以及哪些分区可用于报表。使用 **Settings（设置）> Reporting（报告）> Log Database** 页面可管理 Log Database 操作。

在 Log Database 页面的每个区域单击 **OK（确定）**按钮，以保存并实施在该区域的更改。

更改了一台设备上的 Log Database（日志数据库）设置后，该等更改会应用于您网络中的所有设备。

在页面顶部的 Log Database Location（Log Database 位置）区域输入 Log Database 服务器的 IP 地址 / 实例或主机名称 / 实例。默认情况下将输入安装时创建的 Log Database。如果在产品安装时选择加密数据库连接，则会勾选 **Encrypt connection（加密连接）**复选框。如果在安装期间没有选择加密选项，则可通过勾选此处的复选框来加密数据库连接。

重要事项

要使用加密选项，必须已经将受信任的证书导入到 Log Server 机器中。有关导入受信任的证书的相关信息，请参阅数据库文档。

在安装时创建并在此处显示的其它设置包括：指定的身份验证方法（Windows 或 SQL Server）、用户名及密码。

单击 **Check Status（检查状态）**确定服务器的可用性。

Log Database Options（Log Database 选项）区域的顶部显示活动的 Log Database 名称和 Refresh（刷新）链接。单击 **Refresh（刷新）**可更新 Log Database 页面中显示的信息。请确保在单击 **Refresh（刷新）**前保存设置，因为页面上任何未保存的更改都会清除。

使用 **Settings（设置）> Reporting（报告）> Log Database** 页面的 Database Rollover Options（数据库滚动选项）部分可指定您希望 Log Database 何时创建新的数据库分区，此过程称为“滚动”。

Roll over every（滚动间隔）选项用于指定数据库分区是根据大小 (MB) 还是日期（周或月）滚动。

- 如果是根据大小滚动，请选择 MB 并指定数据库必须达到多少 MB 才开始滚动，范围是 100 - 10240 MB（默认值为 5120）。
- 如果是根据日期滚动，请选择周或月作为测量单位，并且指定数据库分区保留多少全日历周 (1 - 52) 或月 (1 - 12) 后再创建新的分区。

注

如果滚动在一天的忙碌时段开始，在进行滚动处理时性能可能会下降。

为避免出现这种情况，有些环境会选择将自动滚动设置为较长的时期或较大的最大容量。然后，定期执行手动滚动，以防止发生自动滚动。

有关手动滚动的信息，请参阅创建数据库分区（第 138 页）。

请注意，不建议设置超大的个别分区。如果将数据划分到多个较小的分区，报表性能可能会减慢。

创建新的数据库分区时，会自动为该分区启用报表功能（请参阅启用数据库分区（第 139 页））。

单击 **OK（确定）**激活对数据库滚动选项的更改。

配置维护选项

Settings（设置）> Reporting（报告）> Log Database 页面的 Maintenance Configuration（维护配置）区域，用于控制数据库处理的某些方面，例如运行数据库维护作业的时间、某些执行的维护任务、数据库分区和错误日志的删除等。

1. 对于 **Maintenance start time（维护开始时间）**，选择运行数据库维护作业的时间。默认值为 1:00。

   此作业要求的时间和系统资源根据您在此区域选择的任务而有所不同。为尽可能减小对其他活动和系统的影响，最好在电子邮件流量小的时段运行此作业。

2. 勾选 **Automatically delete a partition with an end date older than（自动删除结束日期早于以下日期的分区）**复选框，然后指定分区经多少天（1 到 365）后应予删除。

   警告

   分区删除后，数据无法恢复。有关删除分区的其他方法，请参阅启用数据库分区（第 139 页）。

3. 勾选 **Enable automatic reindexing of partitions on（在下列时间启用自动对分区编制索引）**复选框，然后选择在星期几自动执行此处理（默认值为星期六）。

   重新编制数据库索引对于维护数据库完整性和优化报告速度很重要。

   重要事项

   最好在没有电子邮件流量的时段执行此处理。因为重新编制数据库分区的索引非常耗费资源和时间。在重新编制索引的过程中不应运行报表。

4. 勾选 **Delete failed batches after（在下列时间后删除失败的批次）**复选框，然后输入多少天（1 到 365）后删除失败的批次。默认值为 20。

   如果未勾选此选项，失败的批次会无限期保留，以用于未来处理。

   如果磁盘空间不足或者数据库权限不足，无法将日志记录插入数据库，这些记录就会标示为失败的批次。通常，这些批次在夜间数据库维护作业过程中，会被顺利地重新处理并插入数据库。

   但是，如果不解决磁盘空间或权限问题，这种重新处理无法成功。此外，如果未勾选 **Process any unprocessed batches（处理任何未处理的批次）**选项，则永远不会重新处理失败的批次。它们将会在此处指定的时间过后被删除。

5. 勾选 **Process any unprocessed batches（处理任何未处理的批次）**复选框后，夜间数据库维护作业会重新处理任何失败的批次。

   如果未勾选此选项，则永远不会重新处理失败的批次。它们将在步骤 4 中指定的时间后被删除（如果有）。

6. 勾选 **Delete the log after（在下列时间后删除日志）**复选框，然后输入多少天（1 到 120）后删除数据库错误记录。默认值为 45。

   如果未勾选此选项，则会无限期保留错误日志。

7. 单击 **OK（确定）**激活对维护配置选项的更改。

创建数据库分区

数据库分区存储电子邮件流量活动的个别日志记录。Microsoft SQL Server 用户可以配置 Log Database 根据分区大小或日期间隔创建新的分区（有关详细信息，请参阅配置 *Log Database* 选项（第 135 页））。

如果分区基于大小，所有收到的日志记录都将插入满足大小规则的最近活动分区。当分区达到指定的最大容量时，就会创建新的分区来插入新的日志记录。

如果分区基于日期，新分区会根据确定的周期创建。例如，如果滚动选项为每月，则只要新月份收到记录就会新建一个分区。收到的日志记录根据日期插入相应的分区。

数据库分区具有灵活性和性能优势。例如，您可以从单一分区生成报表，以限制必须进行分析来查找所需信息的数据范围。

Settings（设置）> Reporting（报告）> Log Database 页面的 Database Partition Creation（创建数据库分区）区域用于定义新数据库分区的特性，例如位置和大小选项。此区域还可让您立即创建新分区，而无需等待计划的滚动（请参阅配置 *Log Database* 选项（第 135 页））。

1. 输入文件路径以为新的数据库分区创建数据和日志文件。
2. 在 **Initial Size (MB)（初始大小 (MB)）**下，设置用于新数据库分区的数据及日志文件的初始文件大小（100 到 2048 MB）。

   

   注

   最佳实践建议计算一段时期的平均分区大小。然后将初始大小更新到该值。此方法可将分区扩展次数减至最小，并且释放资源以将数据处理到分区中。

3. 在 **Growth (MB)（增长 (MB)）**下，设置在需要额外空间时分区数据和日志文件的大小增量 (8 - 512 MB)。
4. 单击 **OK（确定）**应用输入的路径、大小和增长更改。

   这些更改后创建的数据库分区将使用新的设置。

5. 单击 **Create（创建）**立即创建新的分区，不受自动滚动设置的影响。

   为使新分区应用在此区域所做的更改，请确保单击 **OK（确定）**后再单击 **Create（创建）**。

   定期单击内容窗格中的 **Refresh（刷新）**链接。Available Partitions（可用的分区）区域在创建过程完成时将显示新的分区。

如果以后更改分区文件路径，应确保对新的数据库文件夹具有写入权限。

启用数据库分区

Settings（设置）> Reporting（报告）> Log Database 页面的 Available Partitions（可用的分区）区域列出可用于报表的所有数据库分区。列表中显示分区的日期范围以及每个分区的大小和名称。

此列表用于控制报表中包含的数据库分区，以及选择要删除的个别分区。

1. 勾选要包含于报表中的每个分区旁边 **Enable（启用）**列中的复选框。

   根据需要使用列表上方的 **Select all（全选）**或 **Select none（全部不选）**选项。

   必须至少启用 1 个分区用于报表。**Select none（全部不选）**选项用于一次禁用所有分区，便于您只启用少数几个分区。

   使用这些选项可管理在生成报表和加速报表处理时必须分析的数据量。例如，如果您计划为六月份生成一系列报表，则只选择包含六月份数据的分区。

   

   重要事项

   此选择会影响计划的报表以及交互运行的报表。为避免生成不含数据的报表，请确保在报表按计划运行时启用相关的分区。

2. 如果不再需要某个分区，请单击该分区名称旁边的 **Delete（删除）**。该分区在下次运行夜间维护作业时将被真正删除。

   

   警告

   请谨慎使用此选项。您无法从已经删除的分区恢复数据。

   删除废弃的分区可以尽量减少 Log Database 中的分区数量，从而改进数据库和报表性能。可根据需要使用这个 Delete（删除）选项删除个别分区。如果要根据时间表删除较早的分区，请参阅配置维护选项（第 137 页）。

3. 单击 **OK（确定）**激活对可用数据库选项的更改。

查看日志活动

Settings（设置）> Reporting（报告）> Log Database 页面的 Log Activity（日志活动）区域用于检查数据库维护状态，以及对 Log Database 运行作业时记录的事件和错误消息。使用 **View（查看）**下拉列表选择显示邮件的最大数量。

更改 Log Database

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在下列任何情况下，可能需要更改 Log Database:

- 数据库 IP 地址改变。
- 数据库用户名和密码改变。
- 用户要更改验证设置。
- 用户要使用具名实例。

此类更改必须在 2 个地方完成: **Settings（设置）> Reporting（报告）> Log Database** 页面和 Email Security Log Server Configuration 向导。

请按照下列步骤更改 Log Database 配置:

1. 在 **Settings（设置）> Reporting（报告）> Log Database** 页面中的 **Log database** 字段中输入新 Log Database 的 IP 地址。
2. 在安装 Log Server 的 Windows 机器上打开 Email Security Log Server Configuration 向导（**开始 > 所有程序 > Websense > Email Security > Email Security Log Server Configuration**）。
3. 在 Database（数据库）选项卡中，单击 **Connection（连接）**打开 Select Data Source（选择数据源）对话框。
4. 选择 Machine Data Source（机器数据源）选项卡，然后单击 **New（新建）**打开 Create New Data Source（创建新的数据源）对话框。
5. 选择 **System Data Source (Applies to this machine only)（系统数据源（仅适用于本机））**，然后单击 **Next（下一步）**。
6. 选择 **SQL Server**，然后单击 **Next（下一步）**。
7. 单击 **Finish（完成）**。
8. 在 Create a New Data Source to SQL Server（创建 SQL Server 的新数据源）对话框中，分别在 **Name（名称）**、**Description（说明）**和 **Server（服务器）**输入字段中输入新 SQL Server 数据库的服务器名称、说明和 IP 地址，然后单击 **Next（下一步）**。
9. 选择 **With SQL Server authentication using a login ID and password entered by the user（使用用户输入的登录 ID 和密码进行 SQL Server 验证）**。
10. 输入用户名 **(sa)** 和密码，然后单击 **Next（下一步）**。
11. 在 **Change the default database to（更改默认数据库）**下拉列表中，选择 **esglogdb76** 数据库，然后单击 **Next（下一步）**。
12. 单击 **Finish（完成）**。
13. 在 ODBC Microsoft SQL Server Setup（ODBC Microsoft SQL Server 设置）对话框中，单击 **Test Data Source（测试数据源）**以测试服务器连接。

14. 单击 **OK（确定）**。
15. 在 SQL Server Login（SQL Server 登录）对话框中输入新的用户名和密码。
16. 在 Email Security Log Server Configuration 向导的 Database（数据库）选项卡中，注意 ODBC Data Source Name (DSN) 字段包含新的服务器名称，然后单击 **Apply（应用）**确认新配置。
17. 在警告消息中单击 **OK（确定）**。Log Server 必须停止并重新启动，新设置才会生效。
18. 在 Email Security Log Server Configuration 向导的 Connection（连接）选项卡中，单击 **Stop（停止）**以停止 Log Server 服务。
19. 在同一选项卡中，单击 **Start（启动）**重新启动 Log Server 服务。新的数据库设置将会生效。

查看 Log Server 设置

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Settings（设置）> Reporting（报告）> Log Server 页面用于查看 Log Server 的 IP 地址或主机名和端口号。单击 **Check Status（检查状态）**确定服务器的可用性。

配置报表首选项

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

报表首选项设置确定如何分发计划的报表以用于检查。您也可以指定计划的报表保留多长时间以及在报表删除前多久提醒管理员。

在一台设备上更改了报表首选项设置后，该等更改会应用于您网络中的所有设备。

使用 **Settings（设置）> Reporting（报告）> Preferences（首选项）**页面，提供通过电子邮件分发完成的已计划报表时所用的信息。此外，也可以定义计划的演示报表存储多长时间后自动删除，以及提前多久提醒管理员报表即将删除。

1. 输入在通过电子邮件分发计划的报表时出现在 From（发件人）字段中的电子邮件地址。
2. 输入在通过电子邮件分发计划的报表时使用的电子邮件服务器的 SMTP 服务器 IP 地址或名称。
3. 使用 **Store reports for（报告存储时长）**下拉列表可指定计划的报告在 Email Security 管理器机器中存储的时间长度（默认为 5 天）。

请注意，报告存储时长的增长会影响所需的 Email Security 管理器机器磁盘空间量。此机器不适合于长期存档报表。

> **注**
> 如果在开始生成报表之后缩短报表存储时间，超过此间隔的已存储报表将会自动删除。

4. 使用 **Give administrators this much warning before a scheduled report is deleted（在计划的报表删除之前提前下列时间提醒管理员）**下拉列表指定在报表删除前多久（1 - 5 天）提醒管理员（默认值为 3 天）。

   提醒的目的是让管理员在重要的报告从 Email Security 管理器机器删除之前将其存档于适当的位置。

5. 单击 **OK（确定）**以应用您的更改。

使用演示报表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

演示报表包含一组预定义的图表和表格式报表模板，可用以生成 Email Security Gateway 消息流量活动的图形报表。您可以运行报表、自定义报表模板或将常用报表标记为“常用”。所有报表既可以立即运行，也可以安排在特定时间或按重复周期运行。

并非所有报表模板都可以自定义。可自定义的报表模板显示的图标与不能自定义的报表不同。如果在选择报表名称时启用了 **Save As（另存为）**按钮，则可保存报表并根据您的需求编辑。如果选择无法自定义的报表，**Save As（另存为）**按钮不会启用。

Main（主要）> Status（状态）> Presentation Reports（演示报表）页面用于根据报表目录中的模板生成图表和表格式报表。

报表目录对一系列预定义的报表模板和自定义报表进行分组。展开一个组可查看其相应的模板和自定义报表。单击模板或报表标题可查看其中内容的简短说明。

要运行演示报表，请在报表目录中选择所需的报表模板，单击 **Run（运行）**，然后按照运行演示报表（第 148 页）中的说明操作。

要使用现有报表作为创建不同报表的模板，请选择自定义报表，然后单击 **Save As（另存为）**（如果此按钮已启用）。如果在选择报表时 Save As（另存为）按钮未启用，便无法编辑模板。有关详细说明，请参阅复制自定义演示报表（第 143 页）。

要使对报表过滤器的更改应用到您创建的任何自定义报表，请在报表目录中选择报表标题，然后单击 **Edit（编辑）**。您无法修改或删除预定义的报表模板。

可将常用报表标记为“常用”，以便更快地找到它们。只需单击报表目录中的报表标题，然后单击 **Favorite（常用）**（请参阅使用常用报表（第 148 页））。勾选 **Show Only Favorites（只显示常用报表）**，只显示报表目录中已标记为常用的模板。

要删除您创建的自定义报表，请单击 **Delete（删除）**。如果删除的报表出现在任何计划的作业中，将继续为该作业生成报表。有关编辑和删除计划的作业的信息，请参阅查看计划的作业列表（第 154 页）。

> **注**
> 在一台设备上对报表设置进行的更改会应用于所有网络设备。

使用页面顶部的按钮可安排报表以后运行、查看计划的报表作业，以及查看和管理计划程序创建的报表。

- 单击 **Job Queue（作业队列）**可查看并管理现有计划作业的列表以及每个作业的状态。请参阅查看计划的作业列表（第 154 页）。
- 单击 **Scheduler（计划程序）**可定义包含一或多个在特定时间或按重复周期运行的报表的作业。请参阅计划演示报表（第 150 页）。
- 单击 **Review Reports（检查报表）**可查看并管理已成功计划和运行的报表列表。请参阅检查计划的演示报表（第 156 页）。

相关主题:

- 复制自定义演示报表（第 143 页）
- 定义报表过滤器（第 144 页）
- 使用常用报表（第 148 页）
- 运行演示报表（第 148 页）
- 计划演示报表（第 150 页）
- 查看计划的作业列表（第 154 页）
- 检查计划的演示报表（第 156 页）

复制自定义演示报表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用 **Save As New Report（另存为新报表）**页面可为自定义报表模板创建可编辑的副本。并非所有模板都可用于创建新的自定义报表。请按照下列步骤复制自定义演示报表:

1. 在报表目录中选择自定义报表，如果 **Save As（另存为）**按钮已启用，请单击此按钮。如果 **Save As（另存为）**按钮未启用，则无法复制和定制所选报表。

2. 在 **Presentation Reports（演示报表）> Save As New Report（另存为新报表）**页面中，将报表目录名称替换为便于识别新报表的名称。（默认名称是原始报表模板的名称，后附数字表示其为副本。）该名称必须是唯一的，最多只能有 85 个字符。
3. 单击 **Save（保存）**或 **Save and Edit（保存并编辑）**。
   - 如果单击 **Save（保存）**，您将返回到 Presentation Reports（演示报表）页面，其中新的报表显示于报表目录中。在任何时间要自定义报表，请选择报表名称，然后单击 **Edit（编辑）**。
   - 如果单击 **Save and Edit（保存并编辑）**，会直接进入 Edit Report Filter（编辑报表过滤器）页面。新报表也会添加到报表目录中。
4. 编辑报表过滤器以修改报表。报表过滤器控制包含于自定义报表中的元素，例如电子邮件发件人或收件人。

   有关说明，请参阅定义报表过滤器（第 144 页）。

定义报表过滤器

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

报表过滤器用于控制报表中包含的信息。例如，您可以选择将报表限于选定的电子邮件发件人、电子邮件收件人或消息扫描结果（例如清洁、病毒、垃圾邮件、商业群发电子邮件或数据安全）。也可以为报表目录中的项目指定新名称和说明、更改报表标题、指定要显示的自定义徽标以及将新报表标记为常用。

> **注**
> 使用自定义徽标需要在定义报表过滤器之前做一些准备工作。您必须以支持的格式创建所需图形并将该文件放置在相应的位置。请参阅自定义报表徽标（第 145 页）。

用于预定义报表模板的过滤器无法更改。在创建自定义报表时，可以在 Save As New Report（另存为新报表）页面中选择 **Save and Edit（保存并编辑）**以编辑其过滤器，或者在任何时候从报表目录中选择该报表，然后单击 **Edit（编辑）**。

Edit Report Filter（编辑报表过滤器）页面包含用于管理报表不同元素的单独选项卡。在每个选项卡中选择所需的项目，然后单击 **Next（下一步）**移至下一个选项卡。有关完成每个选项卡的详细说明，请参阅:

- 设置一般报表选项（第 145 页）
- 选择报表的电子邮件发件人（第 146 页）
- 选择报表的电子邮件收件人（第 146 页）
- 选择报表的邮件扫描结果（第 147 页）

在 Save（保存）选项卡中，选择是要运行还是计划报表，然后保存报表过滤器。请参阅保存报表过滤器定义（第 147 页）。

设置一般报表选项

使用 **Presentation Reports（演示报表）> Edit Report（编辑报表）**页面的 General（一般）选项卡可配置一般报表特性，如下所示:

1. 在 **Report catalog name（报表目录名称）**输入字段中输入新名称，可以修改此报表在报表目录中显示的名称。名称最多可以包含 76 个字符。

   此名称不会出现在报表本身中；只是用于在报表目录中标识报表格式与过滤器的唯一组合。

2. 在 **Report title（报表标题）**输入字段中可修改实际出现在报表中的标题。标题最多可以包含 85 个字符。
3. 使用 **Description（说明）**字段可修改出现在报表目录中的简要报表说明。说明最多可以包含 336 个字符。

   说明应有助于识别报表目录中报表格式与过滤器的这种唯一组合。

4. 使用 **Logo（徽标）**下拉列表指定报表的徽标。默认条目为 **Websense Logo（Websense 徽标）**。如果不想在此报表上显示徽标，请选择 **No Logo（无徽标）**。

   如果已创建并在适当的目录中存储支持的图像文件，则该列表还将包含自定义徽标图像文件的文件名。请参阅自定义报表徽标（第 145 页）。

5. 勾选 **Save as Favorite（另存为常用）**复选框，使报表被选为常用报表。

   报表目录在常用报表旁边显示星号。可以在 Report Catalog（报表目录）页面中选择 Show only Favorites（只显示常用报表），以减少列出的报表数量，便于更快速地移至特定报表。

6. 在所有输入和选择完成后，单击 **Next（下一步）**打开 Senders（发件人）选项卡。

自定义报表徽标

默认情况下，Websense 徽标将显示在演示报表的左上角。在创建自定义报表并编辑其报表过滤器时，可以选择您已经准备好并复制到适当目录中的其他徽标，步骤如下:

1. 以下列格式之一创建图像文件:

   .bmp、.gif、.jfif、.jpe、.jpeg、.jpg、.png、.ttf

   使用最多 25 个字符命名图像文件（包括文件扩展名。）

2. 将图像文件复制到以下默认安装目录中（或复制到您创建的安装目录中）:

   C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\PRTemplate\jasperreports\images

   该目录中所有支持的图像文件将自动出现在 Edit Report Filter（编辑报表过滤器）页面 General（一般）选项卡上的 **Logo（徽标）**下拉列表中。图像将自动缩放以适应分配给徽标的空间。（请参阅设置一般报表选项（第 145 页）。）

选择报表的电子邮件发件人

Presentation Reports（演示报表）> Edit Report（编辑报表）页面的 Senders（发件人）选项卡可让您控制要在报表数据中包含哪些发件人。每个报表只能选择 1 类发件人。

如果要报表所有发件人，则无涯需在此选项卡中选择。

1. 从下拉列表中选择发件人类型。
2. 从 **Search limits（搜索限制）**下拉列表中选择最大搜索结果数 (10 - 1000)。默认值为 10。

   根据您组织的电子邮件流量，Log Database 中可能有大量的用户、组或域。此选项用于管理结果列表的长度，以及显示搜索结果所需的时间。
3. 输入 1 或多个字符进行搜索，然后单击 **Search（搜索）**。

   可使用星号 (*) 作为通配符，表示缺少的字符。例如，J*n 可能返回 Jackson、Jan、Jason、Jon、Joan 等。

   请认真定义搜索字符串，确保所有需要的结果都包含在为限制搜索而选择的数量中。
4. 突出显示结果列表中的 1 或多个项目，然后单击向右箭头按钮 (>) 以将其移至 Selected Senders（选择的发件人）列表中。
5. 按需要重复步骤 2 - 4 以执行其他搜索，并添加更多发件人到 Selected Senders（选择的发件人）列表中。
6. 要从 Selected Senders（选择的发件人）列表中删除一个要目，请选择该条目，然后单击 **Remove（删除）**。
7. 在完成选择或删除之后，单击 **Next（下一步）**打开 Recipients（收件人）选项卡。

选择报表的电子邮件收件人

Presentation Reports（演示报表）> Edit Report（编辑报表）页面的 Recipients（收件人）选项卡，可让您控制要在报表数据中包含哪些收件人。每个报表只能选择 1 类收件人。

如果要报表所有收件人，则无需在此选项卡中选择。

1. 从下拉列表中选择收件人类型。
2. 从 **Search limits（搜索限制）**下拉列表中选择最大搜索结果数 (10 - 1000)。默认值为 10。

   根据您组织的电子邮件流量，Log Database 中可能有大量的用户、组或域。此选项用于管理结果列表的长度，以及显示搜索结果所需的时间。
3. 输入 1 或多个字符进行搜索，然后单击 **Search（搜索）**。

   可使用星号 (*) 作为通配符，表示缺少的字符。例如，J*n 可能返回 Jackson、Jan、Jason、Jon、Joan 等。

   请认真定义搜索字符串，确保所有需要的结果都包含在为限制搜索而选择的数量中。

4. 突出显示结果列表中的 1 或多个项目，然后单击向右箭头按钮 (>) 以将其移至 Selected Recipients（选择的收件人）列表中。
5. 按需要重复步骤 2 - 4 以执行其他搜索，并添加更多收件人到 Selected Recipients（选择的收件人）列表中。
6. 要从 Selected Recipients（选择的收件人）列表中删除一个要目，请选择该条目，然后单击 **Remove（删除）**。
7. 在完成选择或删除之后，单击 **Next（下一步）**打开 Message Scanning Results（邮件扫描结果）选项卡。

选择报表的邮件扫描结果

Presentation Reports（演示报表）> Edit Report（编辑报表）页面的 Message Scanning Result（邮件扫描结果）选项卡，可让您确定在报表中包含哪些电子邮件扫描结果。有以下选择：**Clean（安全）**、**Virus（病毒）**、**Spam（垃圾邮件）**、**Data Security（数据安全）**、**Commercial Bulk（商业群发电子邮件）**、**Custom Content（自定义内容）**、**Block List（阻止列表）**、**Phishing（网络钓鱼）**以及 **ThreatScope**。“阻止列表”类型适用于被 Personal Email Manager 始终阻止列表阻止的邮件。默认选择所有可用的扫描结果。

单击 **Next（下一步）**打开 Save（保存）选项卡。

保存报表过滤器定义

Presentation Reports（演示报表）> Edit Report（编辑报表）页面的 Save（保存）选项卡显示将要出现在报表目录中的名称和说明，并且可让您选择要如何继续。

1. 检查 Name（名称）和 Description（说明）文本。

   如果需要任何更改，请单击 **Back（上一步）**返回到 General（一般）选项卡，在那里可以执行这些更改。在 Save（保存）选项卡中无法编辑名称或说明文本。（请参阅设置一般报表选项（第 145 页）。）
2. 指出您要如何继续：
   - 选择 **Save（保存）**以保存报表过滤器并返回报表目录。
   - 选择 **Save and run（保存并运行）**以保存报表过滤器并打开 Run Report（运行报表）页面。请参阅运行演示报表（第 148 页）。
   - 选择 **Save and schedule（保存并计划）**以保存报表过滤器并打开 Scheduler（计划程序）页面。请参阅计划演示报表（第 150 页）。
3. 单击 **Finish（完成）**以保存报表名称和说明，并实施在步骤 2 中所做的选择。

使用常用报表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以将任何演示报表（模板或自定义报表）标记为常用。使用此选项可以标识您经常生成以及希望能在报表目录中快速找到的报表。

要将报表标记为常用报表:

1. 在 Presentation Reports（演示报表）页面中，在报表目录中选择经常生成或者希望能快速找到的报表。
2. 单击 **Favorite（常用）**。

   列表中的任何常用报表名称在旁边都显示有星号，这样在报表目录显示时便于您快速找到它。
3. 勾选报表目录上方的 **Show Only Favorites（只显示常用报表）**复选框，使列表只显示标记为常用的报表。清除此复选框可恢复报表的完整列表。

如果需要更改，并且常用报表不再常用，可按以下步骤删除常用指定:

1. 选择显示有常用星号的报表。
2. 单击 **Favorite（常用）**。

   星号将从报表目录中的报表名称旁边消除。如果选择 **Show Only Favorites（只显示常用报表）**，该报表将不会出现在列表中。

运行演示报表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用 **Presentation Reports（演示报表）> Run Report（运行报表）**页面可立即生成单一报表。也可以创建包含一或多个报表的作业，并计划它们一次运行或按重复周期运行（请参阅计划演示报表（第 150 页））。

注

在生成 PDF 格式的报表之前，请确保在用于访问 Email Security Gateway 的机器上安装了 Adobe Reader v7.0 或更高版本。

在生成 XLS 格式的报表之前，请确保在用于访问 Email Security Gateway 的机器上安装了 Microsoft Excel 2003 或更高版本。

如果未安装相应的软件，可以选择保存文件。

要运行报表:

1. 在报表目录中选择要运行的报表，然后单击 **Run（运行）**打开 Run Report（运行报表）页面。
2. 选择 **Report date range（报表日期范围）**，定义报表涵盖的时间段。

   如果选择 **Custom（自定义）**，请为报表指定 **Report start date（报表开始日期）**和 **Report end date（报表结束日期）**。
3. 选择报表的**报表输出格式**。

XLS	Excel 电子表格。XLS 文件经过格式化，可重复使用，也可在 Microsoft Excel 中打开。
PDF	可携文档格式。PDF 格式的文件可在 Adobe Reader 中打开。
HTML	超文本标记语言。HTML 格式的文件可在 Web 浏览器中打开。

4. 如果选择了 Top N（前 N 个）报表类型，请选择要报表的项目数。
5. 指定您要如何生成报表:
   - 选择 **Run the report in the background（在后台运行报表）**（默认选择）使报表立即作为计划的作业运行。或者，您也可以提供电子邮件地址，用以在报表完成或无法生成时接收通知邮件。（还可以监控作业队列，了解报表状态。）

     如果在后台运行报表，会自动保存已完成报表的副本，并且报表链接显示在 Review Reports（检查报表）页面中。
   - 取消勾选 **Run the report in the background（在后台运行报表）**将使报表在前台运行。在这种情况下，报表未计划，并且不会出现在 Review Reports（检查报表）页面中。

     如果在前台运行报表，在您关闭用于查看报表的应用程序（例如 Microsoft Excel、Adobe Reader 或 Web 浏览器）时不会自动保存报表，而必须手动保存报表。

注

如果计划在前台运行多个报表，请确保使用嵌入的 **Close（关闭）**按钮关闭用于显示“正在生成报表”和“报表完成”等消息的弹出窗口。如果使用浏览器的关闭 (X) 按钮，以后尝试在前台运行报表可能会失败，除非您离开 Presentation Reports（演示报表）页面后回来再运行报表。

6. 单击 **Run（运行）**。
   - 如果安排报表立即运行，已完成的报表将添加到 Review Reports（检查报表）列表中。要查看、保存或删除报表，请单击 Presentation Reports（演示报表）页面顶部的 **Review Reports（检查报表）**。
   - 如果在前台运行报表，新的浏览器窗口将会出现，显示报表进度。HTML 报表在完成后将显示在浏览器窗口中；您可以选择打开 PDF 或 XLS 格式的报表或者将其保存到磁盘中。
7. 要打印报表，请使用用于显示报表的应用程序所提供的打印选项。

   为获取最佳效果，请生成 PDF 输出以进行打印。然后使用 Adobe Reader 中的打印选项。

计划演示报表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

您可以按需要运行演示报表，或者使用 **Presentation Reports（演示报表）> Scheduler（计划程序）**页面创建作业，以定义运行一个或多个作业的计划。在应用程序群集中，只有主机器才可计划报表。

计划的作业所生成的报表通过电子邮件分发到一个或多个收件人。在创建计划的作业时，请考虑您的电子邮件服务器是否能够处理所附报表文件的大小和数量。

完成的报表也会添加到 **Presentation Reports（演示报表）> Review Reports（检查报表）**页面中（请参阅检查计划的演示报表（第 156 页））。

您可以按下列方式之一访问计划程序:

- 单击 Presentation Reports（演示报表）页面顶部的 **Scheduler（计划程序）**（位于报表目录上方）。
- 编辑报表过滤器时，请在 Save（保存）选项卡中选择 **Save and schedule（保存并计划）**，然后单击 **Finish（完成）**（请参阅定义报表过滤器（第 144 页））。
- 单击 Job Queue（作业队列）页面中的作业名称可编辑作业。
- 单击 Job Queue（作业队列）页面中的 **Add Job（添加作业）**可创建新作业。

Scheduler（计划程序）页面包含多个选项卡，用于选择要运行的报表及其运行时间表。有关完成每个选项卡的详细说明，请参阅:

- 设置计划（第 152 页）
- 选择要计划的报表（第 153 页）
- 设置日期范围（第 153 页）
- 设置输出选项（第 153 页）

在创建作业之后，使用 Job Queue（作业队列）可检查作业状态并查找其他有用的信息（请参阅查看计划的作业列表（第 154 页））。

当计划的演示报表运行后，该报表将作为电子邮件附件发送到收件人。附件名称为报表名称。例如，对于输出格式为 PDF 的报表，附件文件名称可以是 Hybrid Service Messages.pdf。

计划的报表也会自动保存到 Email Security 管理器机器上的报表输出目录（默认为 C:\Program Files (x86)\Websense\Email Security\ESG Manager\tomcat\temp\report\output）。请注意，通过电子邮件发送的附件名称与输出目录中存储的文件名称不匹配。查找特定报表的最佳方法是使用 Review Reports（检查报表）页面，可以按日期或作业名称以及报表名称搜索。

在 **Settings（设置）> Reporting（报告）> Preferences（首选项）**页面中指定的时期（默认为 5 天）过后，报表会自动从 Review Reports（检查报表）页面和报表输出目录中删除。如果要保留报表更长时间，请将其包含在备份例行程序中，或者将其存储到可以长期存储的位置。

在报表删除之前的一段时间内（默认为 3 天），Review Reports（检查报表）页面中会持续显示提醒。使用 **Settings（设置）> Reporting（报告）> Preferences（首选项）**页面可更改此提醒时间。

根据每天生成的报表数量，报表文件可能会占用大量的磁盘空间。请确保 Email Security 管理器机器中具有足够的磁盘空间。如果报表输出目录在文件自动删除之前已经变得过大，您可以手动删除文件。

Websense 软件以您选择的格式生成报表：XLS (Microsoft Excel)、PDF (Adobe Reader) 或 HTML。如果您选择 HTML 格式，报表可能会显示在 Email Security Gateway 内容窗格中。内容窗格中显示的报表无法打印或保存至文件。要打印或保存报表至文件，请选择 PDF 或 XLS 输出格式。

重要事项

要以 PDF 格式显示演示报表，必须在用于访问 Email Security 管理器的机器上安装了 Adobe Reader v7.0 或更高版本。

要以 XLS 格式显示演示报表，必须在用于访问 Email Security 管理器的机器上安装了 Microsoft Excel 2003 或更高版本。

设置计划

在 **Presentation Reports（演示报表）> Scheduler（计划程序）**页面的 Schedule Report（计划报表）选项卡中，计划报表作业一次性完成或按重复的周期进行。

> **注**
> 建议将报表作业安排在不同的日期或不同的时间，以避免 Log Database 超载以及日志记录和交互报表的速度减慢。

1. 在 **Job name（作业名称）**字段中输入唯一标识这个已计划作业的名称。
2. 根据所需的 Recurrence Pattern（重复模式）为作业选择 Recurrence Options（重复选项），如下所示:

重复模式	重复选项
Once（一次）	输入作业运行的确切日期，或者单击图标从日历中选择。
Daily（每天）	没有可用的其他重复选项。
Weekly（每周）	勾选每个要运行作业的周中日期的相应复选框。
Monthly（每月）	输入月中运行作业的日期。日期必须是介于 1 到 31 的数字，且必须用逗号分隔 (1,10,20)。 要在每个月的连续日期运行作业，请输入用破折号分隔的开始和结束日期 (3-5)。

3. 在 Schedule Time（计划时间）框中，设置运行作业的开始时间。

   作业根据运行 Email Security Gateway 的机器上的时间开始。

> **注**
> 要想今天就开始生成计划的报表，请选择足够在开始时间之前完成作业定义的延时。

4. 在 Schedule Period（计划时期）框中，选择开始作业的日期。用于结束作业的选项如下所示:

No end date（无结束日期）	作业根据建立的计划持续无限期运行。 在未来的某个时间要中断作业，请编辑或删除该作业。请参阅查看计划的作业列表（第 154 页）。
End after（结束条件）	选择作业要运行的次数。在运行指定的次数后，作业不再运行，但仍会留在作业队列中，直到您将其删除。请参阅查看计划的作业列表（第 154 页）。
End by（结束日期）	设置作业停止运行的日期。在此日期或之后不会运行。

5. 单击 **Next（下一步）**打开 Select Report（选择报表）选项卡。

选择要计划的报表

使用 **Presentation Reports（演示报表）> Scheduler（计划程序）**页面的 Select Report（选择报表）选项卡可选择用于作业的报表。

1. 在 Report Catalog（报表目录）树中突出显示用于此作业的报表。
2. 单击向右箭头 (>) 按钮可将该报表移至 Selected Reports（选择的报表）列表中。
3. 重复步骤 1 和 2，直到用于此作业的所有报表都出现在 Selected Reports（选择的报表）列表中。
4. 单击 **Next（下一步）**打开 Date Range（日期范围）选项卡。

设置日期范围

使用 **Presentation Reports（演示报表）> Scheduler（计划程序）**页面的 Date Range（日期范围）选项卡设置作业的日期范围。如果在 Schedule Report（计划报表）选项卡中选择了 **Once（一次）**，则 **Specific dates（特定日期）**字段会显示在该选项卡上指定的报表日期。

如果选择了定期报表计划，则可以在 **Relative dates（相对日期）**字段中指定期数（当前、最近、最近 2 个等等），以及时期的类型（日、周，或月）。例如，作业可能涵盖最近 2 周或当前月份。

周代表日历周：星期天至星期六。月代表日历月。例如，“当前周”产生从星期天至今天的报表；“本月”产生从当月第一天至今天的报表；“最近一周”产生从上一个星期天到星期六的报表；依此类推。

在设置作业的日期范围之后，单击 **Next（下一步）**显示 Output（输出）选项卡。

设置输出选项

为作业选择报表之后，使用 Output（输出）选项卡选择输出格式和分发选项。

1. 为完成的报表选择文件格式。

XLS	Excel 电子表格。收件人必须拥有 Microsoft Excel 2003 或更高版本才可查看 XLS 报表。
PDF	可携文档格式。收件人必须拥有 Adobe Reader v7.0 或更高版本才可查看 PDF 报表。
HTML	超文本标记语言。收件人必须拥有 Web 浏览器。

2. 从 **Top N**（前 N 个）下拉列表中选择想要在 Top（排名）格式报表中显示的项目数量。该值的范围为 1 到 200；默认值为 10。
3. 输入用于分发报表的收件人电子邮件地址。

   各个地址之间应该用分号分隔。
4. 此外，您还可以输入电子邮件地址，以通知收件人生成报表失败。

5. 按需要勾选 **Customize subject and message body of notification email（自定义通知电子邮件的主题和正文）**复选框。然后为此作业分发电子邮件输入自定义主题和正文。
6. 单击 **Save Job（保存作业）**以保存和实施作业定义，并且显示 Job Queue（作业队列）页面。
7. 检查此作业及任何其他计划的作业。请参阅查看计划的作业列表（第 154 页）。

查看计划的作业列表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Presentation Reports（演示报表）> Job Queue（作业队列）页面列出为演示报表创建的已计划作业。列表会指示每个作业的状态以及有关作业的信息，例如运行频率。在此页面中可以添加和删除计划的作业、临时暂停作业等。

您可以在页面顶部的 **Job Name（作业名称）**输入字段中输入搜索词来搜索特定作业。单击 **Go（进入）**开始搜索。

单击 **Clear（清除）**删除当前搜索词，然后执行不同的搜索，或者单击页面底部的 **Refresh（刷新）**显示报表的完整列表。

此列表提供每个作业的以下信息:

数据项目	说明
Job Name（作业名称）	创建作业时分配的名称。
Status（状态）	表示作业是否为 • 运行中 • 已计划（等待下次计划的运行时间） • 已成功完成 • 已失败 • 未触发（在上次计划的时间因内存不足或服务器关闭等问题而未运行）
State（状态）	以下状态之一: • **Enabled（已启用）**表示根据现有周期模式运行的作业。 • **Disabled（已禁用）**表示未活动且无法运行的作业。
Recurrence（周期）	为此作业设置的周期模式（一次、每天、每周或每月）。
History（历史记录）	单击 Details（详细信息）链接可打开所选作业的 Job History（作业历史记录）页面。请参阅查看作业历史记录（第 155 页）。
Next Scheduled（下次计划）	下次运行的日期和时间。
Owner（所有者）	计划作业的管理员的用户名称。

Job Queue（作业队列）页面中的选项用于管理作业。有些按钮要求您先勾选每个要包含的作业名称旁边的复选框。

操作	说明
Job name link（作业名称链接）	打开 Scheduler（计划程序）页面，在其中可以编辑作业定义。请参阅计划演示报表（第 150 页）。
Run Now（立即运行）	立即开始运行已在列表中选择的任何作业，不同于计划定期运行的作业。
Add Job（添加作业）	打开 Scheduler（计划程序）页面，在其中可以定义新作业。请参阅计划演示报表（第 150 页）。
Delete（删除）	从作业队列删除在列表中选择的任何作业。作业在删除之后无法恢复。 要临时停止运行特定的作业，请使用 **Disable（禁用）**按钮。
Enable（启用）	重新激活在列表中选择的已禁用作业。作业根据建立的计划开始运行。
Disable（禁用）	中断运行在列表中选择的已启用作业。此选项用于临时暂停您以后可能要恢复的作业。
Refresh（刷新）	以最新的数据更新页面

查看作业历史记录

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

单击 History（历史记录）栏中的 **Details（详细信息）**链接并使用 **Presentation Reports（演示报表）> Job Queue（作业队列）> Job History（作业历史记录）**页面查看关于所选作业近期运行尝试的信息。此页面会单独列出每个作业，其中包含以下信息:

数据项目	说明
报表名称	印在报表上的标题
Start Date（开始日期）	报表开始运行的日期和时间
End Date（结束日期）	报表完成的日期和时间
Status（状态）	指示报表是完成还是失败
Message（消息）	作业的相关信息，例如报表是否成功分发

检查计划的演示报表

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

使用 **Presentation Reports（演示报表）> Review Reports（检查报表）**页面查找、访问和删除计划的报表。默认情况下，报表按照从最新到最早的顺序列出。

要查看列表中的任何报表，请单击报表名称。

- 如果报表是单一的 PDF 或 XLS 文件，可以选择保存或打开报表。这取决于您的浏览器安全设置以及机器上安装的插件。
- 如果报表很大，可能已经保存为多个 PDF 或 XLS 文件并存储在 ZIP 文件中。该文件使用 ZIP 格式压缩。保存 ZIP 文件，然后解压缩其中包含的 PDF 或 XLS 文件以查看报表内容。
- 将鼠标指针停在报表名称旁边的报表图标上，可以查看报表是包含一个还是多个文件。

要将列表限于只显示即将删除的报表，请勾选 **Show only reports due to be purged（只显示即将清除的报表）**复选框。当选择了该选项时，无法使用报表搜索功能。报表存储的时间长度在 **Settings（设置）> Reporting（报表）> Preferences（首选项）**页面中配置（请参阅配置报表首选项（第 141 页））。

要搜索报表列表，请先从 **Filter by（过滤条件）**下拉列表中选择项目，然后输入全部或部分作业名称或日期。请注意，搜索区分大小写。您可以按下列方式搜索:

- 报表或作业名称
- 报表创建日期（创建日期）
- 计划报表的管理员的名称（请求者）
- 报表应删除的日期（清除日期）

单击 **Go（进入）**开始搜索。

单击 **Clear（清除）**删除当前搜索词，然后执行不同的搜索，或者单击 **Refresh（刷新）**显示报表的完整列表。

如果最近完成的报表没有出现在 Review Reports（检查报表）页面中，也可以单击 **Refresh（刷新）**以最新的数据更新页面。

要删除报表，请勾选报表名称旁边的复选框，然后单击 **Delete（删除）**。

要查看已计划报表作业的状态，请单击页面顶部的 **Job Queue（作业队列）**。有关使用作业队列的详细信息，请参阅查看计划的作业列表（第 154 页）。

要计划新的报表作业，请单击 **Scheduler（计划程序）**（请参阅计划演示报表（第 150 页））。

7 配置 Personal Email Manager 最终用户选项

主题:

管理安全套接字层 (SSL) 证书

使用 **Settings（设置）> Personal Email（个人电子邮件）> SSL Certificate（SSL 证书）**页面管理 Personal Email Manager SSL 证书，该证书可确保 Personal Email Manager 设备的电子邮件传输安全。可使用 Personal Email Manager 随附的默认证书，也可以从证书颁发机构 (CA) 导入新的企业证书。

安装 Email Security Gateway 之后，默认证书信息显示在 **Settings（设置）> Personal Email（个人电子邮件）> SSL Certificate（SSL 证书）**页面的 Certificate Details（证书详细信息）部分。详细信息包括证书版本、序列号、颁发机构和到期日期。

导入证书

从 CA 导入 SSL 证书到 Personal Email Manager 以替换当前证书。Personal Email Manager 证书被添加到 Email Security Gateway 管理器时，其信息会自动复制到新设备。

根据以下步骤导入证书:

1. 在 **Settings（设置）> Personal Email（个人电子邮件）> SSL Certificate（SSL 证书）**页面的 Certificate Details（证书详细信息）区域下面，单击 **Import（导入）**。
2. 在确认对话框中单击 **Yes（是）**。Import Certificate（导入证书）区域将显示在 Import（导入）按钮下。
3. 在 **Import Certificate（导入证书）**字段中输入证书文件名，或使用 **Browse（浏览）**找到它。文件格式必须为 .jks、.p12 或 .pfx。
4. SSL 证书文件应使用密码保护。在 **Certificate password（证书密码）**字段中输入密码（最大长度为 100 个字符）。
5. 勾选 **Private key alias（私钥别名）**复选框并在输入字段中输入私钥的可选别名（或标识符）。
6. 勾选 **Private key password（私钥密码）**字段并在输入字段中输入私钥的可选密码（最大长度为 100 个字符）。
7. 单击 **OK（确定）**。
8. 重新启动 Personal Email Manager 服务以激活新证书。

恢复默认证书

通过在 **Settings（设置）> Personal Email（个人电子邮件）> SSL Certificate（SSL 证书）**页面中单击 **Restore Default Certificate（恢复默认证书）**，可随时恢复 Personal Email Manager 的默认证书。此操作将替换当前证书。

应该重新启动 Personal Email Manager 服务以激活新证书。

创建隔离邮件通知邮件

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

Personal Email Manager 通知邮件向用户发出警报，提示发送给用户的电子邮件已被阻止。通知邮件列表包含发送给用户所有电子邮件地址（包括别名地址）的邮件。通知会发送到用户的主要电子邮件地址。

Settings（设置）> Personal Email（个人电子邮件）> Notification Message（通知邮件）页面包括 4 个部分:

- Notification Message Links（通知邮件链接），用于指定 Personal Email Manager 工具最终用户访问的 IP 地址和端口（请参阅指定 *Personal Email Manager* 访问（第 159 页））
- Notification Message Schedule（通知邮件计划），用于设置向用户发送阻止邮件通知的频率（请参阅计划通知邮件（第 160 页））

- Notification Message Template（通知邮件模板），用于编排通知邮件的内容和外观。当用户有被阻止的电子邮件时，他们将在收件箱中看到此邮件。（请参阅使用通知邮件模板（第 160 页）。）
- Recipients List（收件人列表），用于指定接收通知邮件的用户目录。（请参阅创建通知邮件收件人列表（第 161 页）。）

在完成所有 4 个部分后，单击 **OK（确定）**即可传送通知邮件。

指定 Personal Email Manager 访问

使用 Notification Message Links（通知邮件链接）部分指定最终用户用来访问以管理 Personal Email Manager 工具中的阻止邮件的设备。该设置还用于创建用户通知邮件中所列阻止邮件的超链接。您可以根据需要自定义访问 Personal Email Manager 的 URL。

Personal Email Manager 用户必须具有 Personal Email Authentication（个人电子邮件身份验证）权限才能使用该工具。有关授予最终用户 Personal Email Manager 权限的信息，请参阅管理用户验证 / 身份验证选项（第 62 页）。

输入 Personal Email Manager 设备的 IP 地址或主机名。

输入端口号（默认值为 9449）。端口号不能为 Email Security Gateway 或设备保留端口。

> **注**
> 如果使用 C 设备接口访问 Personal Email Manager，则必须使用默认端口 9449。

使用 Custom URL（自定义 URL）字段输入用户访问 Personal Email Manager 的 URL 路径，应不同于使用上面输入的 IP 地址和端口自动生成的路径该 URL 还用于通知邮件的超链接。路径的最大长度为 250 个字母数字字符、连字符和下划线。连字符不能作为第一个字符。自定义 URL 仅支持一个子目录（例如 www.mycompany.com/pemserver），并且应使用在 Port（端口）字段中指定的端口。

部署一组 Email Security 设备来处理 Personal Email Manager 最终用户活动。配置设备集群用于 Personal Email Manager 访问可激活设备的负载均衡功能，从而增强性能。如果所访问的设备已配置在集群中，该设备会通过轮询机制，将 Personal Email Manager 访问请求转发至其他集群机器。

使用 **Settings（设置）> General（一般）> Cluster Mode（集群模式）**页面添加设备和从集群中删除设备（相关信息请参阅配置设备集群（第 52 页））。

计划通知邮件

您可以选择多种方式来计划通知邮件（关于阻止邮件的通知）的频率。在 **Settings（设置）> Personal Email（个人电子邮件）> Notification Message（通知邮件）**中配置计划设置。

在 **Send notifications（发送通知）**下拉列表中选择通知邮件的频率。默认情况下选择 **None（无）**，并且不启用本部分的任何其它选项。

- 如果在 **Send notifications（发送通知）**下拉列表中选择 **Every day（每天）**，则启用 **Time（时间）**选项供用户选择。您可以根据个人意愿选择任意时间间隔（以 1 小时为增量）。
- 如果在 **Send notifications（发送通知）**下拉列表中选择 **Every workday（每个工作日）**，则启用 **Time（时间）**选项供用户选择。您可以根据个人意愿选择任意时间间隔（以 1 小时为增量）。
- 如果在 **Send notifications（发送通知）**下拉列表中选择 **Every week（每周）**，则激活 **Day of week（星期几）**和 **Time（时间）**字段。指定在星期几发送通知邮件。您可以根据个人意愿选择任意时间间隔（以 1 小时为增量）。

> **注**
> 通知邮件只发送给受保护的域。未受保护的域不会收到通知邮件。

使用通知邮件模板

通知邮件模板帮助您确定通知邮件的内容和外观。配置通知邮件如下:

1. 设置每个通知邮件中包括的最大邮件数量。默认值为 50，最大值为 100。如果用户被阻止邮件的数量超过了最大数量，则必须通过通知邮件中的 Web 访问链接直接在 Personal Email Manager 工具中处理额外的邮件。
2. 从以下选项中选择通知要包括的电子邮件操作:
   - **Not Spam（非垃圾邮件）**（默认选择），允许用户报告被阻止的邮件不应归为垃圾邮件
   - **Deliver（传送）**（默认选择），允许用户解除对邮件的阻止。电子邮件也许会直接传送到用户的收件箱，或者提交给后续过滤器继续进行处理（如适用）。所采取的操作由 **Settings（设置）> Personal Email（个人电子邮件）> End-user Portal（最终用户门户）**页面上 Quarantined Message Delivery Options（隔离邮件投递选项）部分的设置决定。
   - **Delete（删除）**（默认选择），从用户的被阻止邮件列表中删除被阻止的邮件
   - **Add to Always Block list（添加到“始终阻止”列表）**，允许经授权的用户添加地址到个人的 Always Block（始终阻止）列表
   - **Add to Always Permit list（添加到“始终允许”列表）**，允许经授权的用户添加地址到个人的 Always Permit（始终允许）列表
3. 在 **Company（公司）**输入字段中输入您的公司名称及其他相关信息。

4. 在 **Description（说明）**输入字段中输入电子邮件过滤产品的简要说明（默认为“Websense Email Security Gateway”）。
5. 在 **Sender（发件人）**字段中输入通知邮件的发件人电子邮件地址。
6. 在 **Subject（主题）**字段中配置通知邮件显示的主题行。当用户收到通知邮件时，该主题将显示在用户收件箱中。
7. 在 **Header（标题）**字段中指定通知邮件的适当标题文本。默认为“The following messages are isolated”（以下邮件被隔离）。
8. 在 **Footer（页脚）**字段中指定通知邮件的适当页脚文本。默认为“For more information, contact your administrator”（有关详细信息，请联系管理员）。

创建通知邮件收件人列表

通过在 Recipients List（收件人列表）部分输入用户的详细信息，可确定接收通知邮件的 Personal Email Manager 用户。只有 Recipients（收件人）列表中列出的用户才会收到有关被阻止邮件的通知邮件。

Recipients（收件人）列表基于用户目录。所有现有用户目录列在用户目录框的左侧。选择用户目录并单击右箭头可将该目录添加到 **Recipients（收件人）**列表。

在 Add User Directory（添加用户目录）页面单击 **Add user directory（添加用户目录）**以创建新目录（有关详细信息，请参阅添加和配置用户目录（第 54 页））。在创建新用户目录后，它将显示在 Notification Message（通知邮件）页面的用户目录列表中。

如果要从 Recipients（收件人）列表中删除用户目录，请在 Recipients（收件人）列表中选择该目录，然后单击 **Delete（删除）**。

设置用户帐户选项

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

在 **Settings（设置）> Personal Email（个人电子邮件）> User Accounts（用户帐户）**页面中可以配置部分 Personal Email Manager 用户帐户选项。该页面允许用户管理个人的 Always Block（始终阻止）和 Always Permit（始终允许）列表，将被阻止邮件的管理任务委托给其他个人，以及在单个 Personal Email Manager 会话中管理多个用户帐户。

在一台设备上进行的用户帐户管理配置设置会应用于您网络中的所有设备。

授权使用阻止和允许列表

授权用户在登录 Personal Email Manager 后可管理其个人的 Always Block（始终阻止）和 Always Permit（始终允许）列表。使用 **Settings（设置）> Personal Email（个人电子邮件）> User Accounts（用户帐户）**页面指定可管理个人阻止和允许列表条目的用户。

添加授权用户

通过指定其用户具有 Personal Email Manager 身份验证权限的用户目录，可允许用户管理其个人的 Always Block（始终阻止）和 Always Permit（始终允许）列表。在 User Directories（用户目录）页面创建用户目录，然后在 Add User Authentication（添加用户身份验证）页面中指定这些用户目录的身份验证选项。（有关用户目录的详细信息，请参阅添加和配置用户目录（第 54 页）；有关用户身份验证设置的信息，请参阅管理用户验证 / 身份验证选项（第 62 页）。）

在 **Settings（设置）> Personal Email（个人电子邮件）> User Accounts（用户帐户）**页面中，已指定 Personal Email Manager 权限的用户目录显示为可用用户目录。要授予用户目录组管理个人阻止 / 允许列表的权限，请通过勾选目录名称旁边的复选框选择可用目录列表中的用户目录，然后单击箭头按钮将其移动到 Recipients（收件人）框。

删除授权用户

通过在 Recipients（收件人）框中选择用户目录并单击 **Delete（删除）**，可删除此前授权的用户。该用户目录仍然显示在可用目录框中，但其成员不再具有 Always Block/Always Permit（始终阻止 / 始终允许）列表的管理权限。

启用用户帐户管理

在 **Settings（设置）> Personal Email（个人电子邮件）> User Accounts（用户帐户）**页面中勾选 **Enable user account management（启用用户帐户管理）**复选框，可以为 Personal Email Manager 最终用户启用用户帐户管理功能：您可以允许最终用户将被阻止邮件的管理任务委托给其他 1 人或多人。

最终用户可以在 Personal Email Manager 最终用户界面的 User Account Access（用户帐户访问）页面中配置这些选项。有关详细信息，请参阅 *Personal Email Manager 用户帮助*。

自定义 Personal Email Manager 最终用户门户

Email Security Manager 帮助 | 电子邮件安全解决方案 | 7.8.x 版

可使用 **Settings（设置）> Personal Email（个人电子邮件）> End-user Portal（最终用户门户）**页面自定义最终用户工具的外观和指定其邮件显示在 Personal Email Manager 最终用户通知电子邮件中的隔离邮件队列。

选择徽标显示

默认情况下，Websense 公司名称和徽标显示在 Personal Email Manager 最终用户页面上。用户可以选择在门户上不显示任何公司名称或徽标。为此，请将 Company name（公司名称）字段留空，并在 Logo（徽标）字段下拉列表中选择 **None（无）**。

您还可以自定义最终用户门户，让您的公司名称和徽标显示在那里。使用以下步骤可在 End-user Portal Options（最终用户门户选项）部分自定义您的 Personal Email Manager 最终用户门户:

1. 在 **Company name（公司名称）**字段中输入您的公司名称。
2. 在 Logo（徽标）字段下拉列表中，选择 **Custom（自定义）**。
3. 这时将出现 **Upload logo（上传徽标）**字段。浏览到所需的徽标文件并选择它进行上传。徽标文件必须为:
   - .gif、.png、.jpeg 或 .jpg 文件格式
   - 最大 1 MB 和 120 x 34 像素

通过单击徽标文件名旁边的 **Browse（浏览）**并浏览到新的徽标文件，可更改所使用的徽标文件。

启用被阻止邮件传送

指定您希望将被 Personal Email Manager “始终阻止”列表阻止的邮件传送至的队列。

勾选 **Save the original message to a queue（将原始邮件保存到队列）**复选框，然后从下拉列表中选择一个队列，或为其添加一个新队列。

启用最终用户操作审计

指定是否要保持从 Personal Email Manager 通知邮件或隔离邮件列表执行的最终用户电子邮件管理活动的记录。

在 End-user Audit Option（最终用户审计选项）部分勾选 **Audit end-user actions（审计最终用户操作）**复选框，以启用 Personal Email Manager 审计日志。在 **Main（主页）> Status（状态）> Logs（日志）> Personal Email Manager** 下查看该日志。有关该日志的信息，请参阅 *Personal Email Manager 审计日志*（第 26 页）。

激活隔离邮件列表缓存

可为 Personal Email Manager 最终用户隔离邮件列表激活列表缓存功能，以便通过减少数据库刷新操作的次数来增强列表显示性能。以下最终用户操作不会自动触发页面刷新:

- Delete（删除）
- Deliver（传送）
- Reprocess（重新处理）
- Not spam（非垃圾邮件）

当自动刷新发生时，这些操作可减小隔离邮件列表的大小，直到页面小于其原始大小的一半。

Personal Email Manager 最终用户可随时通过单击 **Refresh（刷新）**来启动手动页面刷新。

选择隔离邮件队列显示

通过在 Message Queue Display Settings（邮件队列显示设置）部分勾选所需队列名称旁边的复选框，选择要对 Personal Email Manager 最终用户显示的邮件队列。

启用隔离邮件传送

可以指定当最终用户对隔离邮件列表中的选定邮件单击 **Deliver（传送）**时，Personal Email Manager 做出的行为。选择以下选项之一:

- **Deliver quarantined message（传送被隔离的邮件）**，允许最终用户解除对电子邮件的阻止，将其直接传送到他们的收件箱。
- **Resume quarantined message processing（继续处理隔离邮件）**，强制对被阻止的电子邮件进行分析，继续经过所有后续过滤器的处理。若使用此选项，如果邮件触发后续过滤器，则可能不会传送给最终用户。

索引

C

D

E

F

G

H

I

J

K

L

M

P

Q

R

S

T

U

V

W

X

Y

Z