

具有DMZ的MeetingPlace Web现场安装

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Components Used](#)

[Conventions](#)

[验证的项目，在您去现场前](#)

[检验连通性](#)

[单击出席考虑事项](#)

[验证的项目，在您开始现场工作前](#)

[检验连通性](#)

[分组在MeetingTime设置的默认](#)

[MeetingPlace Web安装](#)

[现场的工作以后的验证条目](#)

[测验公众大会](#)

[测验会议](#)

[测验演讲样式会议](#)

[Web会议和通知验证](#)

[Introduction](#)

本文略述验证程序为使用，在您去现场前，或者，在您开始现场工作前，并且，在您完成与非敏感区域(DMZ)后现场工作的所有Cisco MeetingPlace Web。

[Prerequisites](#)

[Requirements](#)

确认您读了[Cisco MeetingPlace Web版本注释版本5.3](#)，并且需求符合。不同的部署模型需求，被分段满足Access-1服务器(SMA-1S)和被分段满足Access-2服务器(SMA-2S)在页被找到六和七thr版本注释文档。

[Components Used](#)

本档中的信息基于以下软件和硬件版本：

- Cisco MeetingPlace Web版本5.3
- DMZ体系结构(DMZ-B和DMZ-C) — (这些指SMA-1S和SMA-2S在[管理员指南Cisco MeetingPlace Web会议版本的5.3](#) — 设立和配置。)

[Conventions](#)

有关文档规则的详细信息，请参阅 [Cisco 技术提示规则](#)。

[验证的项目，在您去现场前](#)

在您去现场前，此部分概述必要的验证步骤。

[检验连通性](#)

完成这些步骤：

1. 查看在[管理员指南](#)的章节5 [Cisco MeetingPlace](#)看待如何的[Web会议版本的5.3](#)与安全套接字层SSL设置一起配置外部Web会议。
2. 验证端口80或端口443 (SSL协议)是开放的从互联网和对DMZ服务器。
3. 验证端口80是开放的从内联网和对互联网。
4. 验证端口5003是开放的在DMZ服务器和Cisco MeetingPlace服务器(Cisco MeetingPlace网关系统完整性模块[GWSIM]之间使用此)。从DMZ服务器起动到内联网
5. 对于WebShare，如果要避免建立隧道，请确保您有端口1627开放从互联网和对DMZ服务器。从互联网起动到DMZ服务器如果此端口不是开放的，则通过端口80或443使用隧道，是更加慢十的百分比。
6. 对于WebShare，请确保您有端口1627开放从内联网和对DMZ服务器，如果要避免建立隧道。从内联网起动到DMZ服务器如果此端口不是开放的，则通过端口80或443使用隧道，是更加慢十的百分比。
7. 仅对于NetMeeting，请验证您有端口1503开放从互联网和对DMZ服务器。从互联网起动到DMZ服务器
8. 仅对于NetMeeting，请验证您有端口1503开放从内联网和对DMZ服务器。从内联网起动到DMZ服务器

[单击出席考虑事项](#)

设想这些要素：

1. 能使用一被分段的(或拆分)域名系统(DNS)？这在您的通知允许您使用单个URL。
2. 否则，您必须决定如何修改通知模板：是否计划使用两个URL？是否计划使用基于的不同的URL会议是否公共或私有？
3. 确认您是否有最终用户试验测试功能在安装或升级以后。
4. 是否使用或计划使用NT验证？

[验证的项目，在您开始现场工作前](#)

[检验连通性](#)

完成这些步骤：

1. Ping和NSLOOKUP (如果开放)内部网络服务器的完全合格的域名(FQDN)或IP地址从另一个内部PC的。Ping meetingplace.company.com (请用服务器的正确主机名替换)NSLOOKUP

meetingplace.company.com (请用服务器的正确主机名替换)**Note:** 使用NSLOOKUP，打开DOS提示符(请去Start > Run，输入cmd并且点击OK键)，然后输入NSLOOKUP meetingplace.company.com (请用服务器的正确主机名替换)。

2. Ping和NSLOOKUP (如果开放) DMZ Web服务器的FQDN或IP地址从外部PC的。
3. Ping和NSLOOKUP (如果开放) DMZ Web服务器的FQDN或IP地址从另一个内部PC的。
4. Ping和NSLOOKUP (如果开放) MeetingPlace服务器的FQDN或IP地址从DMZ Web服务器的。
5. 在端口5003的Telnet从DMZ Web服务器到Cisco MeetingPlace服务器。遵从这些步骤确认端口是开放的：去Start > Run并且输入telnet servername 5003命令，其中servername是MeetingPlace服务器的名称或IP地址，并且点击OK键。如果看到一系列的无意义的字符(例如，☺♥，☹/v[\ ? π [\ ? ýç)，端口5003是开放的。输入Ctrl-] (控制，正确托架)退出。如果获得失败的连接，如显示此处，则端口5003不是开放的：

```
Could not open connection to the host, on port 5003: Connection failed
```

在MeetingTime设置的组默认

什么是预定会议多数常见的类型？

Note: 如果预定会议主要内部，设置满足对大家功能的组默认显示对不。如果他们的主要公众大会，则见面对大家的集显示对是。

MeetingPlace Web安装

完成这些步骤(这些步骤变化基于他们是否适用于一或服务器配置)：

1. 验证服务器的硬件与软件硬件要求。确保在网关机器的硬件符合所有适当要求。主机更多会议的计算机必须有更加快速，更加好的硬件。
2. 对于SMA-1S部署，请遵从步骤实施的在表5-1和2服务器部署的被分段的会议访问的，参考表5-2在[Cisco MeetingPlace Web会议版本的5.3管理员指南](#)。

现场的工作以后的验证条目

测验公众大会

确认以下各项：

1. 验证这些能力：请使用内部网站登陆作为配置文件的用户。要安排公共会议，请使用内部网站。要安排一公共会议用附件，请使用内部网站。您能查看从内部PC的附件。您接收上述会议的通知。出席链路工作的单击内部地。出席从互联网PC的链路工作的单击。内部和外部阅读器能加入Web会议，以及共享和在同一个Web会议合作。
2. 确认这些能力和限制在外部站点：当您从内部站点时，出席您登陆作为您的配置文件。您能访问附件和幻灯片从外部服务器。访客不能添加附件或更改权限或者用户显示选项。

Note: 如果会议室看上去冻结在一百分比或，如果会议室功能变灰，可能不正确地输入主机名或DMZ模板当前没有使用外部会议重定向。

测验会议

完成这些验证步骤。

1. 验证这些能力：您能从内部网站安排私人会议。您能查看从内部PC的此私人会议。您能从内部网站安排一私人会议用附件。您能查看从内部PC的附件。您接收上述会议的通知。出席链路工作的单击内部地。内部查看器能加入Web会议。
2. 验证这些限制：您不能出席从DMZ网站的一私人会议。当您加入Web会议时，您没有重定向到DMZ网站。

[测验演讲样式会议](#)

完成这些验证步骤。

1. 验证这些能力：您能从内联网安排公共和私有演讲样式会议。配置文件的用户能召开从内联网和互联网的演讲样式会议。配置文件的用户允许从内联网和互联网协作。
2. 验证这些访客限制：访客不能召开从内联网的演讲样式会议。访客不能召开从互联网的演讲样式会议。访客没有允许从内联网协作。访客没有允许从互联网协作。

Web会议和通知验证

完成这些验证步骤。

1. 验证隧道，如果端口1627不是开放的：Web管理员用户用户接口的(UI)洛金。**Cisco MeetingPlace Web**的洛金。**Admin**链路在欢迎使用页的右上。点击**数据会议服务器**链路。点击**先进的**链路。检查**强制HTTP隧道**方框。点击**加入Web会议按钮**。如果WebShare客户端打开("欢迎到MeetingPlace应用程序Sharing.")，建立隧道是工作。如果WebShare客户端不打开，建立隧道不是工作。您应该[与思科技术支持联系](#)。
2. 验证通知正确地被派出，并且出席的单击链路工作。