ICS 35.040
L 80

中华人民共和国国家标准

GB/T 30278—2013

信息安全技术
政务计算机终端核心配置规范

Information security technology—Chinese government desktop core configuration specifications

2013-12-31 发布　　2014-07-15 实施

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

知识星球https://t.zsxq.com/JmiaeUR

知识星球https://t.zsxq.com/JmiaeUR

目　　次

知识星球https://t.zsxq.com/JmiaeUR

知识星球https://t.zsxq.com/JmiaeUR

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本标准起草单位:国家信息中心、中国信息安全测评中心、中国信息安全认证中心、国家税务总局电子税务管理中心、三零卫士公司、北京北信源软件股份有限公司、天津市信息中心、上海市信息中心、山西省经济信息中心、江苏省信息中心、安徽省经济信息中心、山东省信息中心、河南省信息中心、湖南省人民政府经济研究信息中心、广东省发展和改革委员会信息中心、四川省经济信息中心、贵州省信息中心、甘肃省信息中心、青海省信息中心、新疆维吾尔自治区经济信息中心、宁波市信息中心、西安市信息中心。

本标准主要起草人:李新友、刘蓓、许涛、蔡军霞、刘帅、程浩、王啸天、沈大风、吴亚非、袁志强、张海昆、刘海峰、甘杰夫、李建彬、闵京华、林浩、王华峰、陆小敏、马志红、谷和启、彭云峰、洪之民、宋苏宇、柳松、马占飞、余靖浊、袁继会、闫加元、靳力、赵俊、史小列、阮高峰。

知识星球https://t.zsxq.com/JmiaeUR

知识星球https://t.zsxq.com/JmiaeUR

信息安全技术
政务计算机终端核心配置规范

1 范围

本标准规定了政务计算机终端核心配置的基本概念和要求，核心配置的自动化实现方法，规范了核心配置实施流程。

本标准适用于政务部门开展计算机终端的核心配置工作。涉密政务计算机终端安全配置工作应参照国家保密局相关保密规定和标准执行。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 22239—2008 信息系统安全等级保护基本要求

3 术语和定义

下列术语和定义适用于本文件。

3.1

政务部门 government department

从事涉及政府性事务工作的国家机关、企事业单位和大型社会团体等机构。

3.2

核心配置项(配置项) core configuration item

计算机操作系统、办公软件、浏览器、BIOS 系统和防恶意代码软件等基础软件中影响计算机安全的关键参数可选项。

注：核心配置项类型包括开关项、枚举项、区间项和复合项，可以根据安全要求对其进行赋值。

3.3

核心配置 core configuration

对核心配置项进行参数设置的过程。

注：通过核心配置限制或禁止存在安全隐患或漏洞的功能，启用或加强安全保护功能，来增强计算机抵抗安全风险的能力。

3.4

核心配置项基值 core configuration item base value

按照核心配置基本要求对配置项的参数设置。

3.5

核心配置基线 core configuration baseline

能够满足计算机安全基本要求的一组核心配置项基值构成的集合。

3.6

核心配置清单 core configuration list

由核心配置项构成的一种列表，是对核心配置项属性的一种形式描述。

知识星球https://t.zsxq.com/JmiaeUR

3.7

核心配置基线包　core configuration baseline package

为实现核心配置基线自动化部署而制定的一种具有特定语法格式的核心配置数据文件。

4　缩略语

下列缩略语适用于本文件。

BIOS:基本输入输出系统(Basic Input Output System)

CGDCC:政务计算机终端核心配置(Chinese Government Desktop Core Configuration)

FTP:文件传输协议(File Transfer Protocol)

GUID:全球唯一标识符(Globally Unique Identifier)

TCM:可信密码模块(Trusted Cryptography Module)

WMI:桌面管理规范(Windows Management Instrumentation)

XML:可扩展置标语言(Extensible Markup Language)

5　概述

5.1　核心配置对象

本标准针对应用于政务部门的联网计算机终端提出核心配置要求,包括连接到互联网、政务专网(政务内网、政务外网)的桌面计算机、膝上型计算机和瘦客户机等。

5.2　核心配置范围

核心配置的范围包括如下方面:

a)　操作系统,如 Windows 系列、国外 Linux 和国产 Linux 等;

b)　办公软件,如国外 Office 软件和国产 WPS 软件等;

c)　浏览器软件,如国外 Internet Explore、Chrome、Firefox 和国产遨游、360 浏览器等;

d)　邮件系统软件,如国外 Outlook 和国产 Foxmail 等;

e)　BIOS 系统软件,如 AMI BIOS、Award BIOS 等;

f)　防恶意代码软件,如内防病毒、防木马软件等。

依据 GB/T 22239—2008 中 7.1.3 和 7.1.4 对于第三级主机安全和应用安全的要求,上述基础软件应符合如下配置要求:

a)　身份鉴别:包括账户登录和口令管理;

b)　访问控制:包括账户管理和权限分配;

c)　安全审计:包括账户行为审计和资源访问审计;

d)　剩余信息保护:包括临时文件、历史文件和虚拟文件管理;

e)　入侵防范:包括对组件的保护功能开启、应用程序的更新升级;

f)　恶意代码防范:包括杀毒软件的安装、升级和病毒查杀管理;

g)　资源控制:包括服务、端口、协议等资源管理和数据的加密保护。

5.3　核心配置项基本类型

根据核心配置项的取值范围,核心配置项分为开关项、枚举项、区间项和复合项等基本类型。

a)　开关项:取值仅为“0”或“1”。例如,配置项“下载未签名的 Active 控件”,可赋值为“启用(1)”或“禁用(0)”。

知识星球https://t.zsxq.com/JmiaeUR

b) 枚举项：取值是离散的、可数的且多于两种。例如，配置项“具有从网络访问本地计算机权限的账户”，可赋值为“管理员(Administrators)”“超级用户(Power Users)”“一般用户(Users)”或“来宾(Guests)”。

c) 区间项：取值连续分布在一个区间内。例如，配置项“账户锁定时间”，赋值范围为“1 min～99 999 min”。

d) 复合项：由上述两种或多种关联配置项组合而成。例如，配置项“启动屏幕保护程序的等待时间”，由开关项和区间项组成。首先“启用”屏幕保护程序，再设置“等待时间”。

5.4 核心配置项赋值方法

根据核心配置项赋值路径不同，可分为注册表赋值和配置文件赋值两种方法：

a) 注册表赋值方法

通过修改核心配置项对应的注册表键值等，实现对配置项的赋值，例如 Windows 操作系统。

b) 配置文件赋值方法

通过修改配置文件中有关的配置项，实现对配置项的赋值，例如 Linux 操作系统。

根据核心配置部署方式不同，可分为手动和自动两种方法：

a) 手动赋值

对核心配置项进行人工逐项赋值。该方法适用于针对少量终端的少量配置部署。例如，在 Windows 系统环境下，运行组策略编辑器(GPEdit)，由人工对核心配置项进行赋值；在 Linux 系统环境下，直接编辑配置文件，对核心配置项逐项进行赋值；在 BIOS 系统中，直接在人机界面上，逐项进行手动赋值。

b) 自动赋值

编辑核心配置基线包，调用自动部署工具，对核心配置项进行赋值。该方法适用于大量终端批量配置部署。

5.5 核心配置对安全的作用

核心配置主要通过如下四种方式提高终端安全性：

a) 应启用数字签名、数据执行保护(DEP)、加密存储、更新升级等安全保护功能；

b) 应禁用存在或可能存在安全漏洞的服务、端口、程序、脚本和驱动等；

c) 应加强口令管理、身份鉴别、账户管理和安全审计等安全保护手段；

d) 应限制软硬件访问权限、资源共享和远程登录等功能。

5.6 核心配置自动化实施框架

核心配置自动化实施框架包括以下四个部分：

a) 提出核心配置基本要求，根据计算机终端所属系统或环境的安全需求及安全级别，确定核心配置具体要求。核心配置基本要求见第 7 章。

b) 编制核心配置清单，采用清单方式描述核心配置要求，包括配置项标识、配置项名称、配置项组别、安全级别、取值范围、配置项基值、赋值路径和检查规则等。核心配置清单格式要求见第 8 章。

c) 生成核心配置基线包，将配置清单转化成为一种符合 XML 语法的嵌套式结构数据文件，以供自动化部署工具实施。核心配置基线包格式要求见第 9 章。

d) 自动部署及监测，通过搭建核心配置自动化部署平台，实现核心配置项的批量自动赋值和合规性实时检测。具体技术要求见第 10 章。

知识星球https://t.zsxq.com/JmiaeUR

6 核心配置基本要求

6.1 操作系统核心配置要求

6.1.1 概述

本标准依据 GB/T 22239—2008 中 7.1.3 对第三级主机安全的要求，针对国内外主流操作系统，在身份鉴别、访问控制、安全审计、剩余信息保护、入侵防范和资源控制等方面提出核心配置基本要求。

6.1.2 身份鉴别

身份鉴别配置要求包括：

a) 账户登录时，应启动身份验证机制，限制连续登录失败次数，连续多次登录失败后应锁定账户；

b) 应配置安全的口令长度、复杂度、有效期和加密强度，应禁止不设置口令；

c) 启动账户登录界面时，应禁止无关进程的启动和运行，防止鉴别信息被窃听。

注：附录 A 给出了身份鉴别配置要求示例。

6.1.3 访问控制

访问控制配置要求包括：

a) 应禁用匿名账户(Anonymous)、来宾账户(Guest)、产品支持账户(Support)，限用管理员账户(Administrator)，重命名管理员账户，限制普通用户的访问权限，禁止任何账户远程访问；

b) 应限制账户对文件、硬件、驱动、内存和进程等重要资源的访问权限；

c) 应限制账户权限提升和授权访问等操作。

6.1.4 安全审计

安全审计配置要求包括：

a) 应启用安全日志，记录账户的创建、更改、删除、启用、禁用和重命名等操作，记录账户登录和注销、开关机、配置变更等操作；

b) 应启用系统日志，记录对文件、文件夹、注册表和系统资源的访问操作。

6.1.5 剩余信息保护

剩余信息保护配置要求包括：

a) 关闭系统时，应清除虚拟内存页面文件；

b) 断开会话时，应清除临时文件夹；

c) 应禁止剪贴板存储信息与远程计算机共享。

6.1.6 入侵防范

入侵防范配置要求包括：

a) 应启用资源管理器数据执行保护(DEP)模式和 Shell 协议保护模式；

b) 打开邮件的附件时，应启用杀毒软件进行扫描；

c) 应启动屏幕保护和休眠功能，设置唤醒口令；

d) 应开启系统定期备份功能；

e) 应限制应用程序的下载和安装，保持操作系统补丁及时更新。

6.1.7 资源控制

资源控制配置要求包括：

知识星球https://t.zsxq.com/JmiaeUR

a) 应禁用信息共享、动态数据交换(Dynamic Data Exchange)、互联网信息服务(Internet Information Services)、FTP 和 Telnet 等网络连接、远程网络访问等服务,限制蓝牙等无线连接;
b) 应禁止介质自动运行(Auto run);
c) 应关闭 FTP、HTTP(超文本传输协议 Hypertext Transport Protocol)、RPC(远程过程调用协议 Remote Procedure Call Protocol)、UPNP(通用即插即用 Universal Plug and Play)、远程桌面服务、远程控制类软件服务端监听、木马软件等对应开放的端口;
d) 应禁止 IPC(进程间通信 Inter Process Communication)管道连接,限制 SYN(同步字符 Synchronize)的传输次数和发送时间;
e) 应启用磁盘加密系统等数据保密配置。对于三级以上政务计算机应配置 TCM 模块保护敏感数据。

6.2 办公软件核心配置要求

依据 GB/T 22239—2008 中 7.1.4 对第三级应用安全的要求,针对国内外主流办公软件提出如下核心配置要求:

a) 应禁止 ActiveX 控件的使用;
b) 应禁用所有未经验证的加载项;
c) 应限用未数字签名的宏;
d) 应限制在线自动更新升级、网上下载剪贴画和模板等资源,以及访问超级链接。

6.3 浏览器核心配置要求

6.3.1 概述

依据 GB/T 22239—2008 中 7.1.4 对第三级应用安全的要求,针对国内外主流浏览器,在浏览器安全选项、域安全管理和隐私保护等方面提出核心配置基本要求。

6.3.2 浏览器安全选项

浏览器安全选项配置要求包括:

a) 应严格禁止运行 java 小程序脚本;
b) 应限制下载和安装未签名的 Active X 控件;
c) 应开启浏览器的保护模式。

6.3.3 域安全管理

域安全管理配置要求包括:

a) 访问以太网的安全限制应设为中或高;
b) 访问企业专网的安全限制可设为中;
c) 访问可信站点的安全限制可设为低;
d) 应限制访问受限站点,禁止从受限站点下载或保存文件。

6.3.4 隐私保护

隐私保护配置要求包括:

a) 退出网页时,应删除 Cookie 文件、下载记录、访问网站历史记录和临时文件夹;
b) 应限制输入框自动关联功能。

6.4 邮件系统核心配置要求

依据 GB/T 22239—2008 中 7.1.4 对第三级应用安全的要求,针对国内外主流邮件系统软件提出如

知识星球https://t.zsxq.com/JmiaeUR

下配置要求：

a） 应配置安全的邮箱登录口令的长度和复杂度；

b） 对本地存储的邮件应开启加密功能；

c） 发送邮件应使用数字签名和数字加密技术，接收邮件应对数字签名进行验证；

d） 应开启加密协议收发邮件；

e） 应禁止直接运行附件中存在安全隐患的文件类型；

f） 应禁止运行邮件中的超链接；

g） 应启用垃圾邮件过滤功能。

6.5 BIOS 系统核心配置要求

依据 GB/T 22239—2008 中 7.1.3 对第三级主机安全的要求，对 BIOS 系统提出如下配置要求：

a） 开机时应启动身份鉴别机制，并设置安全的口令长度和复杂度；

b） 应限制硬件资源使用，包括软驱、硬盘、内存、USB 设备、网卡和 CPU 等；

c） 应启用硬盘写保护；

d） 应限制使用定时开机、远程模式控制开机、键盘鼠标开机等开机模式；

e） 操作系统操作关机后，应立即断开计算机电源；

f） 应限制由外部设备，如 U 盘、光驱等引导启动计算机终端。

6.6 防恶意代码软件核心配置要求

防恶意代码软件核心配置要求包括：

a） 应开启实时保护功能；

b） 应及时升级防恶意代码软件至最新版本，开启自动更新病毒库功能；

c） 应定期进行病毒、木马等恶意代码扫描，发现恶意代码立即隔离或删除。

7 核心配置清单

7.1 概述

核心配置清单描述配置项的属性，包括配置项标识、配置项名称、配置项描述、配置项组别、安全级别、取值范围、配置项基值、赋值路径和检查规则。

7.2 配置项属性

7.2.1 配置项标识

配置项标识是配置项的唯一编码，由三组字符构成，通过“-”进行分隔，标识规则如图 1 所示。最高组位的字符使用 CGDCC，代表政务终端核心配置；中间组位引用软件产品标识；最低组位使用 4 位数字代表配置项序号。例如“Window7 口令长度”配置项，其标识为“CGDCC-win7-0011”。

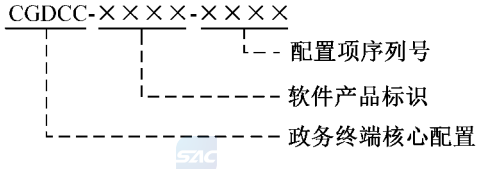

图 1 配置项标识规则

知识星球https://t.zsxq.com/JmiaeUR

7.2.2 配置项名称

描述配置项名称的字符串。

7.2.3 配置项描述

从终端的安全风险、配置项的应对措施和潜在影响等三个方面对配置项进行解释说明。其中，安全风险主要描述配置项所对应的系统脆弱性；应对措施主要描述配置项推荐参数赋值；潜在影响主要描述配置生效后可能对终端系统造成的影响。

7.2.4 配置项组别

需对配置项进行分组时，描述配置项所属的组别。

7.2.5 安全级别

描述配置项对计算机终端安全性的影响程度，分为一般、重要和严重三个级别。

7.2.6 取值范围

描述配置项允许赋值的范围，可用开关、枚举和区间表示。

7.2.7 配置项基值

描述符合核心配置基本要求的配置项基值。当配置项安全级别为严重时，此配置项必须按照基值进行赋值。

7.2.8 赋值路径

描述配置项的赋值路径。对于 Windows 的配置项，可以依据配置项的赋值路径，使用相应的配置工具进行赋值。例如，配置项“账户锁定时间”的赋值路径为“Computer Configuration\Windows Settings\Security Settings\Account Policies\Account Lockout Policy”，通过组策略编辑器(GPEdit)工具，在该路径下可对“账户锁定时间”进行赋值。

7.2.9 检查规则

描述检查配置项的实际值是否达到基值的判断规则，如大于配置项基值、小于配置项基值、等于配置项基值、大于或等于配置项基值、小于或等于配置项基值。

8 核心配置基线包

8.1 概述

核心配置基线包是一种嵌套式结构的数据文件，采用 XML 格式对核心配置基线中各配置项的属性进行规范性标记，以实现核心配置部署及监测的自动化。

核心配置基线包由格式版本标记、基线标记和产品标记三部分组成。其中，基线标记包括基线版本标记、配置组标记、配置项标记和检查标记。核心配置基线包格式结构如图 2 所示。

知识星球https://t.zsxq.com/JmiaeUR

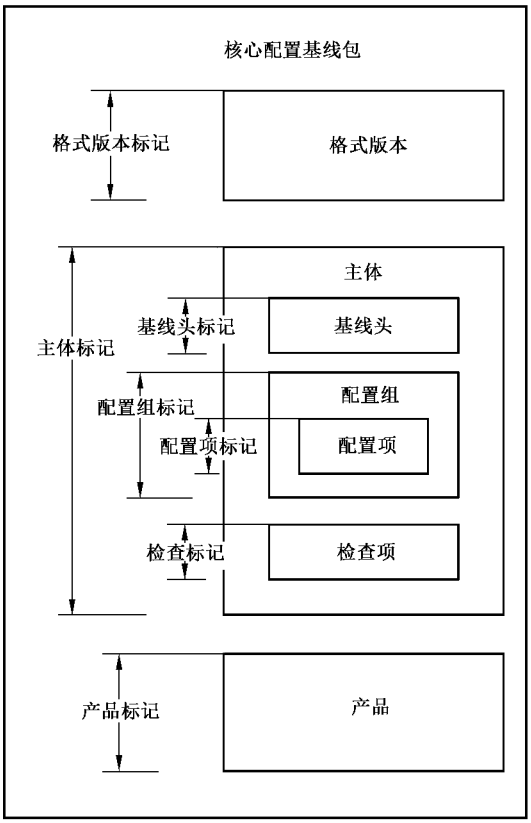

图 2　核心配置基线包格式结构

8.2　主标记

核心配置基线包用“CGDCC-Package”作为主标记，其结构如表 1 所示。

表 1　主标记

标记	名称	解释说明
CGDCC-FormatInfo	格式版本信息	描述核心配置基线包格式的基本信息
CGDCC-Baseline	基线信息	描述核心配置基线的完成信息，可以描述多条基线
CGDCC-Product	产品信息	描述软件产品基本信息，可以描述多个产品信息
示例： 〈CGDCC-Package〉 〈CGDCC-FormatInfo〉……〈/CGDCC-FormatInfo〉 〈CGDCC-Baseline〉……〈/CGDCC-Baseline〉 〈CGDCC-Baseline〉……〈/CGDCC-Baseline〉 …… 〈CGDCC-Product〉……〈/ CGDCC-Product〉 〈CGDCC-Product〉……〈/ CGDCC-Product〉 …… 〈/ CGDCC-Package〉		

8.3　格式版本标记

格式版本用“CGDCC-FormatInfo”作为标记，描述核心配置基线包格式版本的基本信息，其结构如

知识星球https://t.zsxq.com/JmiaeUR

表 2 所示。

表 2　格式版本标记

标记	名称	解释说明
Version	版本编号	核心配置基线包规则版本的唯一标识
Description	概要介绍	对版本规则进行简要说明
示例： 〈CGDCC-FormatInfo〉 〈Version Minor="0" Major="1"/〉 〈Description〉此格式专用于核心配置基线包，版本为 1.0。〈/Description〉 〈/CGDCC-FormatInfo〉		

8.4　基线标记

8.4.1　基线主标记

用“CGDCC-Baseline”作为基线主标记，描述核心配置基线的基本信息，其结构如表 3 所示。

表 3　基线标记

标记	名称	解释说明
Name	基线名称	描述核心配置基线名称
ID	基线标识	描述核心配置基线唯一标识。此标识按照唯一标识(GUID)生成规则自动生成
RevisionNumber	基线修订版本次数	描述核心配置基线的修订版本号，并与 ID 一起可用来追溯基线的修订过程
Version	基线版本	描述所生成核心配置基线的版本
Mode	基线状态	包括可编辑状态和已发布状态两种
VersionControl	版本控制	描述核心配置基线版本相关信息
SettingGroup	配置组信息	描述核心配置基线所包含的每个策略组的基本信息，可包括多个基线组
Check	检查信息	描述策略组所包含的核心配置项的检查信息，每个配置项都有一条相应的检查信息
ProductID	基线所属产品标识	描述该核心配置基线所属的软件产品标识，用于基线适用性检查
示例： 〈CGDCC-Baseline　Name="CGDCC-Win7-v1.0" ID="{0ff11dd2-2186-4670-939d-968347e81558}"〉 〈RevisionNumber〉0〈/RevisionNumber〉 〈Version Minor="0" Major="1"/〉 〈Mode〉Edit〈/Mode〉 〈VersionControl〉……〈/VersionControl〉 〈SettingGroup〉……〈/SettingGroup〉 …… 〈Check〉……〈/Check〉 …… 〈ProductID〉{1739795a-9a4f-4032-b8db-8834dba5a0ea}〈/ProductID〉 〈/CGDCC-Baseline〉		

知识星球https://t.zsxq.com/JmiaeUR

8.4.2 配置项组别标记

用“SettingGroup”作为配置项组别标记，描述配置项分类的基本信息，其结构如表 4 所示。

表 4 配置项组别标记

标记	名称	解释说明
Name	配置项组别名称	描述配置项组别的名称
ID	配置项组别标识	描述配置项组别的唯一标识(GUID)
Description	配置项组别描述	描述配置项组别的功能介绍
Version	配置项组别版本	描述配置项组别的版本序号
SettingItem	配置项信息	描述配置项的基本信息，可以包含多个配置项
示例： 〈SettingGroup Name＝"账户锁定策略组" ID＝"{f74636ac-0619-4be7-ac00-6ae9887707b6}" 〈Description〉……〈/Description〉 〈Version Minor＝"0" Major＝"1"/〉 〈SettingItem〉……〈/ SettingItem〉 …… 〈SettingItem〉……〈/ SettingItem〉 〈/ SettingGroup〉		

8.4.3 配置项标记

8.4.3.1 配置项主标记

用“SettingItem”作为配置项标记，描述各核心配置项的基本信息，如表 5 所示。

表 5 配置项标记

标记	名称	解释说明
Name	配置项名称	描述配置项的名称
ID	配置项标识	描述配置项的唯一标识(GUID)
Content	配置项内容	描述配置项内容，包括：赋值路径、脆弱性、应对措施、潜在影响等，详见 8.4.3.2
DiscoveryInfo	配置项取值	描述配置项取值类型，包括：作用范围、取值方式、取值数据类型等，详见 8.4.3.3
ExportInfo	配置项赋值	描述配置项赋值的过程，包括组策略导出文件类型、导出文件中配置项的名称等，详见 8.4.3.4
示例： 〈SettingItem Name＝"账户锁定时间"ID＝"{7ddcb250-58ff-452b-8b38-bafa8b782675}"〉 〈Content〉…….〈/Content〉 〈DiscoveryInfo〉……〈/DiscoveryInfo〉 〈ExportInfo〉……〈/ExportInfo〉 〈/SettingItem〉		

知识星球https://t.zsxq.com/JmiaeUR

8.4.3.2 配置项内容标记

8.4.3.2.1 配置项内容主标记

用“Content”作为配置项内容标记，描述各核心配置项内容的主要信息，如表 6 所示。

表 6 配置项内容标记

标记	名称	解释说明
Description	介绍	描述配置项功能及相关参数
UIPath	赋值路径	描述配置项的赋值具体路径
Vulnerability	脆弱性	描述该配置项所对应的系统脆弱性
CounterMeasure	应对措施	解决如何对配置项参数正确赋值
PotentialImpact	潜在影响	说明启用配置项后可能会造成不确定的影响
ValueRange	取值范围	允许配置项赋值的范围
Unit	计量单位	配置项参数的计量单位
ValueMappingTable	取值映射表	如果配置项的参数是几个可枚举值，比如是代表颜色的红(0xFF0000)、绿(0x00FF00)和蓝(0x0000FF)，括号内为真正取值，此表描述取值与代表此值的显示名称的映射关系，可帮助用户在界面上对取值进行指定
示例： 〈Content〉 〈Description〉本配置项内容的解释〈/Description〉 〈UIPath〉计算机配置\Windows 设置\安全设置\账户策略\账户锁定策略〈/UIPath〉 〈Vulnerability〉对本配置项的解决的脆弱点进行描述。〈/Vulnerability〉 〈Countermeasure〉使用配置项建议的描述。〈/Countermeasure〉 〈PotentialImpact〉采用配置项后所带来的潜在风险描述。〈/PotentialImpact〉 〈ValueRange High="99999"Low="0"〉〈/ValueRange〉 〈Unit〉分钟〈/Unit〉 〈ValueMappingTable〉……〈/ValueMappingTable〉 〈/Content〉		

8.4.3.2.2 配置项取值映射表标记

用“ValueMappingTable”作为配置项取值映射表标记，描述核心配置项取值映射表的主要信息，如表 7 所示。

表 7 取值映射表标记

标记	名称	解释说明
Mapping	一个映射	描述一个取值和与之相对应的显示名称的对应关系
DisplayName	显示名称	取值相对应的显示名称
Value	值	配置项真正取值

知识星球https://t.zsxq.com/JmiaeUR

表 7（续）

标记	名称	解释说明
示例： 〈ValueMappingTable〉 〈Mapping DisplayName="Enabled" Value="1" /〉 〈Mapping DisplayName ="Disabled" Value="0" /〉 …… 〈/ValueMappingTable〉		

8.4.3.3 配置项取值标记

用“DiscoveryInfo”作为配置项取值标记，描述核心配置项取值方法，如表 8 所示。

表 8 配置项取值标记

标记	名称	解释说明
Scope	作用范围	指配置项作用范围：本机(Machine)或当前账户(User)
DiscoveryType	取值方式	描述配置项的取值方式，包括 WMI、注册表等
DataType	取值数据类型	描述配置项取值的数据类型，比如，整型、字符串
WMIDiscoveryInfo	WMI 取值信息	描述值在 WMI 中的位置
RegistryDiscoveryInfo	注册表取值信息	描述值在注册表中的位置
ScriptDiscoveryInfo	脚本取值信息	描述用来取值的脚本

示例：

例 1(注册表类型)：

```
〈DiscoveryInfo〉
  〈SettingDiscoveryInfo DiscoveryType="Registry" Scope="Machine"〉
    〈RegistryDiscoveryInfo〉
      〈mssasc-core:Hive〉HKEY_LOCAL_MACHINE〈/mssasc-core:Hive〉
      〈mssasc-core:DataType〉REG_DWORD〈/mssasc-core:DataType〉
    〈mssasc-core:KeyPath〉System\CurrentControlSet\Services\LanManServer\Parameters〈/mssasc-core:KeyPath〉
      〈mssasc-core:ValueName〉enableforcedlogoff〈/mssasc-core:ValueName〉
    〈/RegistryDiscoveryInfo〉
  〈/SettingDiscoveryInfo〉
  〈DataType〉Int64〈/DataType〉
〈/DiscoveryInfo〉
```

例 2(WMI 类型)：

```
〈DiscoveryInfo Scope="Machine" DiscoveryType="WMI" DataType="Int64"〉
  〈WMIDiscoveryInfo〉
      〈cgdcc-core:Namespace〉root\rsop\computer〈/cgdcc-core:Namespace〉
      〈cgdcc-core:Class〉RSOP_SecuritySettingNumeric〈/cgdcc-core:Class〉
      〈cgdcc-core:Property〉Setting〈/cgdcc-core:Property〉
      〈cgdcc-core:Where〉KeyName='LockoutDuration' Andprecedence=1〈/cgdcc-core:Where〉
  〈/WMIDiscoveryInfo〉
〈/DiscoveryInfo〉
```

注：cgdcc-core 是命名空间的前缀。

知识星球https://t.zsxq.com/JmiaeUR

8.4.3.4 配置项赋值标记

用“ExportInfo”作为配置项赋值标记，描述核心配置项赋值方法，如表 9 所示。在组策略工具中，通过加载组策略导出文件(GPO Backup)进行赋值。

表 9 配置项赋值标记

标记	名称	解释说明
GPOGenerateFormat	组策略导出文件类型	描述组策略导出文件的类型，包括 INF、CSV、POL 三种类型
Inf Name	导出文件中配置项的名称	组策略导出文件中描述配置项的名称
SectionName	导出文件中的段名称	组策略导出文件中描述配置项所在的段的名称
示例： 〈ExportInfo GPOGenerateFormat="INF"〉 〈Inf Name="LockoutDuration" SectionName="SystemAccess"/〉 〈/ExportInfo〉		

8.4.4 配置项检查标记

用“Check”作为配置项检查标记，描述判断配置项是否存在，以及实际值是否达到基值的规则，如表 10 所示。

表 10 配置项检查标记

标记	名称	解释说明
SettingRef	配置项标识引用	描述所要检查配置项的标识
ExistentialRule	配置项存在规则	检查配置项是否存在
ValidationRules	配置项有效规则	检查配置项参数是否符合规定

示例：

```
〈Check〉
  〈SettingRef setting_ref="{7ddcb250-58ff-452b-8b38-bafa8b782675}"/〉
  〈ExistentialRule Name="Account lockout duration" Value="0" Operator="GreaterThan" Severity="Important"〉
    〈Description〉Win7，Vista，and XP have the same duration.Their environment set to 15 minutes.〈/Description〉
  〈/ExistentialRule〉
  〈ValidationRules〉
    〈SettingRule Name="Account lockout duration" Operator="Equals" Severity="Informational"〉
      〈Description〉The setting does this by specifying the number of minutes a locked out account will remain unavailable.If the value for this policy setting is configured to 0，locked out accounts will remain locked out until an administrator manually unlocks them.〈/Description〉
      〈Value Value="15"/〉
    〈/SettingRule〉
  〈/ValidationRules〉
〈/Check〉
```


知识星球https://t.zsxq.com/JmiaeUR

8.5 产品标记

用“CGDCC-Product”作为配置基线的产品标记，描述配置基线适用产品的主要信息，如表 11 所示。

表 11 产品标记

标记	名称	解释说明
ID	产品标识	描述软件产品的唯一标识(GUID)
DisplayName	产品名称	描述软件产品的名称
OperatingSystemInfo	操作系统版本	描述操作系统的版本号。 此项与 MsiInfo 项、PlatformApplicabilityCondition 项为三选一
MsiInfo	产品安装信息	描述软件产品的安装信息
PlatformApplicability-Condition	适用环境信息	描述软件产品适用的操作系统
ProductFamilyRef	产品所属家族	描述软件产品所属的产品系列的总称，如 Windows。用 GUID 标识表示

示例：

例 1(操作系统)：

```
〈CGDCC-Product ID="{1739795a-9a4f-4032-b8db-8834dba5a0ea}" DisplayName="Windows7"〉
  〈OperatingSystemInfo BuildVersion="7600" MinorVersion="1" MajorVersion="6"/〉
  〈ProductFamilyRef productfamily_ref="{5cea53d1-8a08-4804-8886-1ddea5899aea}"/〉
〈/CGDCC-Product〉
```

例 2(应用软件)：

```
〈Product DisplayName="Microsoft Office 2007 SP2"
ID="{90120000-002C-0409-0000-0000000FF1CE}"〉
    〈MsiInfo ProductCode="{90120000-002C-0409-0000-0000000FF1CE}" IsPerUser="false" /〉
    〈ProductFamilyRef productfamily_ref="{e73048d6-ea6b-45d6-9218-d49404fda64e}" /〉
〈/Product〉
```

9 核心配置自动化部署及监测技术要求

9.1 自动化部署及监测平台基本架构

对于有一定规模的政务终端核心配置应用，需要配备自动化部署及监测平台，进行核心配置编辑、验证、部署和监测。自动化部署及监测平台由四个基本功能模块构成，分别是配置编辑模块、配置验证模块、配置部署模块和配置监测模块，如图 3 所示。其中，配置编辑模块主要用于将核心配置清单自动转换生成核心配置基线包，配置验证模块用于对核心配置基线包进行验证和测试，生成可部署的配置基线包；配置部署模块用于对核心配置基线包进行自动化部署；配置监测模块用于对核心配置状态进行自动监测。

知识星球https://t.zsxq.com/JmiaeUR

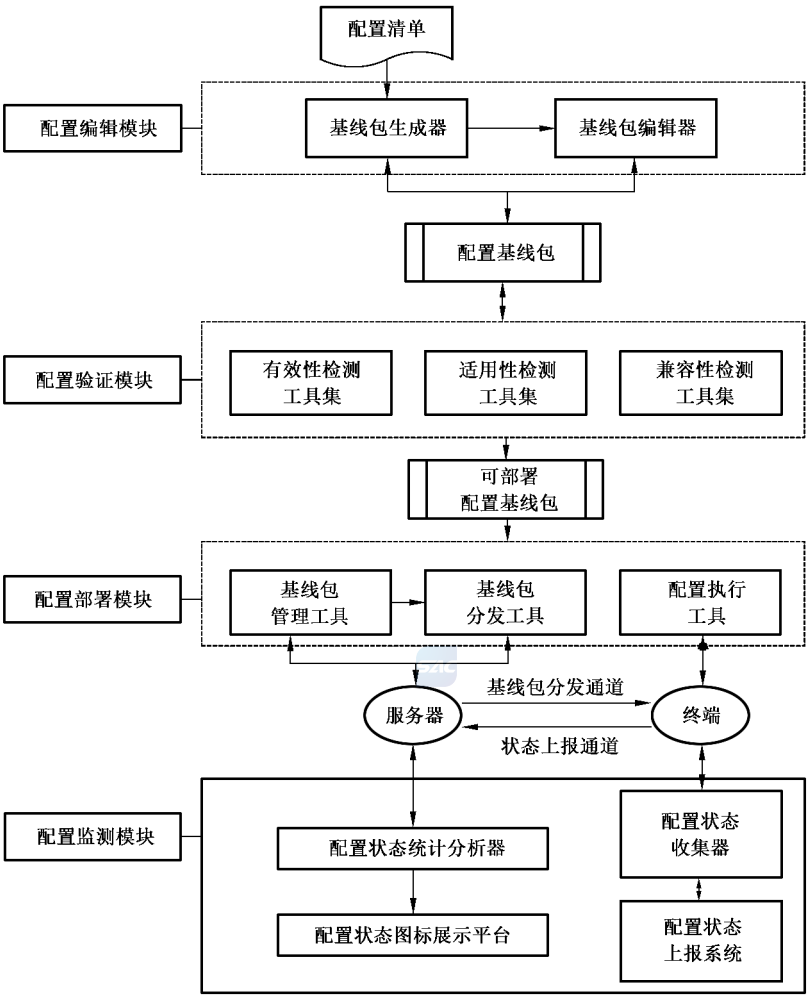

图 3　自动化部署及监测平台

9.2　配置编辑模块

配置编辑模块用来生成核心配置基线包，安全管理员依照核心配置基本要求制定配置清单，并对其进行转换和处理，生成可以编辑、可以解析、可以分发和可以部署的核心配置基线包。配置编辑模块应包括基线包生成器和基线包编辑器两个部件：

a）　基线包生成器主要用于生成原始的核心配置基线包，可根据清单内容逐项录入或由清单模版自动录入；

b）　基线包编辑器主要用于修改核心配置基线包中的配置项的基值，并可进行添加、修改、合并、删除等编辑操作。

9.3　配置验证模块

配置验证模块用于验证核心配置基线包的有效性、适用性和兼容性，保证所要部署的配置基线包的实施效果和安全。

有效性测试可采用人工测试与工具测试相结合的方法，验证核心配置基线包是否生效。具体要求包括：

a）　核心配置部署前，自动收集测试终端的脆弱性情况；

知识星球https://t.zsxq.com/JmiaeUR

b） 核心配置部署后，检测核心配置项的实际赋值是否与基值相一致；

c） 对测试终端进行渗透测试，检验核心配置项是否发挥安全作用。

兼容性测试用于测试核心配置项之间的兼容性，解决终端核心配置项之间的冲突问题。具体要求包括：

a） 支持核心配置项的分析对比，找出有冲突的核心配置项；

b） 可修改存在兼容性问题的核心配置项。

适用性测试用于评估核心配置基线对终端应用环境的影响，包括功能影响、性能影响、系统异常风险等。具体要求包括：

a） 能够收集测试终端软硬件环境信息，识别操作系统版本，以及已安装的应用程序；

b） 能够针对具体的配置项，检查其影响范围，识别出受其影响的软件清单及其原因；

c） 能够识别异常现象，追溯其产生的原因，定位相关配置项；

d） 支持多用户环境下的适用性测试，支持常用软件和业务应用软件的适用性测试。

9.4 配置部署模块

配置部署模块可进行核心配置基线包管理、分发和部署执行，由基线包管理工具、基线包分发工具和配置执行工具三个部分组成。

a） 基线包管理工具具备核心配置基线包上载、内容查看、网络分发，以及基线包更新和删除等功能；

b） 基线包分发工具将基线包按照 IP 或部门区域定向分发到客户端，可采用服务器推送和客户端相结合的分发模式；

c） 配置执行工具自动解析配置基线包赋值方法和路径，并对配置项进行参数赋值，赋值前应对注册表及相关配置文件进行备份，然后在系统（System）权限下执行赋值过程。

9.5 状态监测模块

状态监测模块是安全管理员掌握全网终端核心配置状况的一个重要手段，主要由安装在终端上的配置状态收集器、配置状态上报工具和部署在服务器上的配置状态分析器、配置状态图展示平台组成。

a） 配置状态收集器定时收集终端的核心配置项参数设置情况；

b） 配置状态上报系统用于将收集的配置状态上传至服务器；

c） 配置状态分析器用于对上报的配置状态与核心配置基线进行比对和统计分析；

d） 配置状态图展示平台通过图、表等展示手段输出配置状态分析结果。

10 实施流程

10.1 实施流程框架

政务计算机终端核心配置实施流程主要包括实施准备、基线制定、测试验证、配置部署、配置检查和例外处理等六个阶段，如图 4 所示。

知识星球https://t.zsxq.com/JmiaeUR

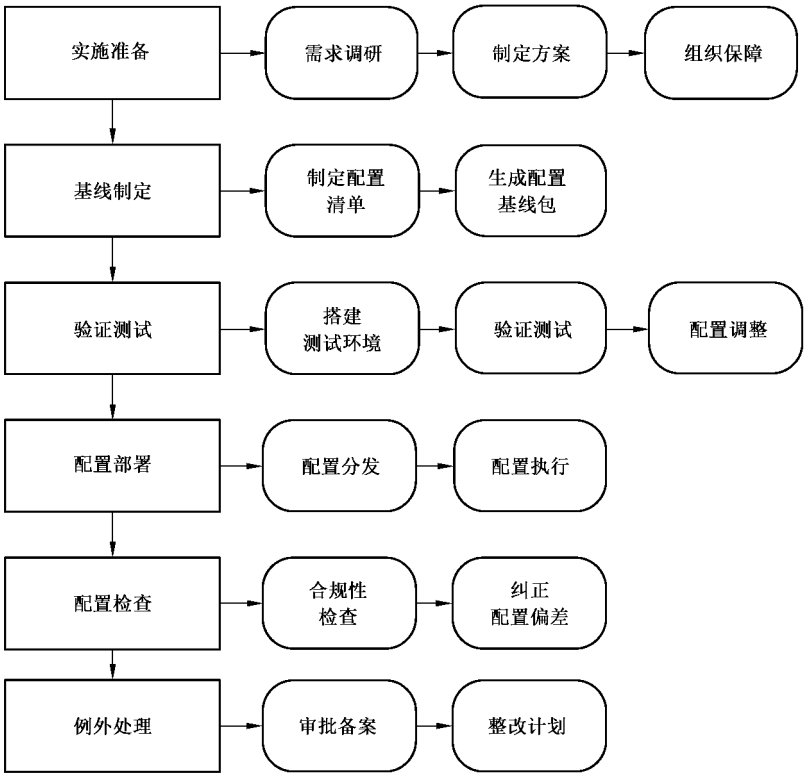

图 4　实施流程

10.2　实施准备

10.2.1　概述

本环节重点从技术和管理两个方面做好实施前准备，主要步骤包括：

a）　需求分析和调研；

b）　制定总体实施方案；

c）　建立组织管理架构，制定相关管理制度，提供组织保障。

10.2.2　需求调研

通过调研网络终端的分布、软硬件资产配备及应用情况，分析政务部门安全目标和安全需求，从而确定实施终端核心配置的目标、范围和基本要求，并评估核心配置实施可能带来的风险。

10.2.3　制定方案

制定政务部门实施终端核心配置总体工作计划，指导后续开展的工作，方案的主要内容包括：

a）　工作计划：各阶段的具体工作计划，包括工作内容、工作形式、工作成果等内容；

b）　进度计划：核心配置实施的时间进度安排；

c）　平台搭建技术方案：规模应用条件下，应搭建核心配置自动化部署及监测平台。应制定平台建设技术方案，并在实施前完成平台搭建工作。

10.2.4　组织保障

组建由领导层、管理层、相关业务骨干和安全技术人员构成的实施团队。必要时，可聘请相关专业

知识星球https://t.zsxq.com/JmiaeUR

的技术专家和技术骨干组成专家小组，指导实施过程。

组织核心配置技术培训和保密教育，制定核心配置管理制度，明确工作职责和任务，得到政务部门最高管理者的支持和批准，必要时签署个人保密协议。

10.3 基线制定

10.3.1 概述

本环节主要根据政务部门确定的核心配置基本要求，制定核心配置清单，并利用核心配置自动化部署及监测平台生成核心配置基线包。

10.3.2 制定配置清单

在第7章提出的核心配置基本要求的基础上，制定符合政务部门安全目标和安全要求的核心配置清单，其格式应符合本标准第8章的规定。

附录B列举了身份鉴别配置要求对应的核心基线配置清单示例。

10.3.3 生成配置基线包

将配置清单内容逐项录入基线包生成器或者利用清单模板自动录入，可生成原始的核心配置基线包，然后在此基础上进一步筛选配置项或者调节配置项基值，生成用于部署的核心配置基线包。

10.4 验证测试

10.4.1 概述

本环节主要目标是验证测试核心配置基线包的有效性、适用性和兼容性，尽量避免首次部署核心配置基线所可能引发新的安全风险。本阶段的主要工作包括：

a) 搭建验证测试环境；
b) 对核心配置基线包进行有效性、适用性和兼容性测试；
c) 对存在问题的核心配置项参数进行重新设置。

10.4.2 搭建测试环境

从验证核心配置基线包的有效性、适用性及兼容性的需求出发，搭建验证测试环境。主要部署必要的硬件设备和测试工具软件，模拟终端的实际运行环境。

10.4.3 验证测试过程

利用核心配置自动化部署及监测平台的配置验证模块分别进行核心配置有效性、适用性和兼容性验证测试，记录测试结果，定位存在问题的核心配置项。

10.4.4 配置调整

对存在有效性、适用性或兼容性问题的核心配置项参数进行修改和调整，重新生成用于部署的核心配置基线包。原则上配置项的赋值不应低于基值。

10.5 配置部署

10.5.1 概述

本环节主要完成核心配置基线包的分发和本地执行过程。可采用自动部署方式和手动部署方式。

知识星球https://t.zsxq.com/JmiaeUR

10.5.2 配置分发

通过核心配置自动化部署及监测平台在一定的网络范围内，自动分发核心配置基线包。可以面向不同安全域，不同 IP 地址段，或者不同部门进行定向分发。

10.5.3 配置执行

利用配置部署模块的客户端，或以手工方式，或镜像方式在本地计算机终端执行核心配置项赋值过程。一般部署核心配置基线包前，应备份当前计算机终端的配置状态，以便部署过程中出现问题时可以及时恢复。

10.6 配置检查

10.6.1 概述

核心配置部署完成后定期进行配置状态检查是保证终端始终处于安全状态的重要手段。本环节的工作重点是进行核心配置合规性检查，并及时纠正存在偏差的配置项参数值。

10.6.2 合规性检查

合规性检查主要检查终端核心配置状态是否达到核心配置基线要求，可以定期（如每月或每周一次）进行检查，或者通过部署核心配置状态监测模块进行实时监测，以保证终端核心配置状态达标。

10.6.3 纠正配置偏差

核心配置部署完成后，在实际运行过程中配置项值可能会由于软硬件环境变化、系统调试需要，或人为原因等发生改变，与配置项基值存在偏差，一般是低于配置项基值。此情况下，应及时重新部署核心配置基线，纠正配置偏差。

10.7 例外处理

10.7.1 概述

政务部门首次部署核心配置基线时，应充分考虑到不同终端在软硬件资产配备方面的差异性。如，个别终端的操作系统版本过低，不适用于部署核心配置基线，或者发生软硬件不兼容的情况，均应作为例外处理。关键步骤包括审批备案和制定整改计划。

10.7.2 审批备案

例外主要分如下三种情况：

a） 无法部署核心配置基线；

b） 可以部分部署；

c） 需调低某些核心配置项值后进行部署。

安全管理员应及时将例外终端软硬件环境信息、例外原因、处理方法等报告领导层进行审批备案。经过审批的例外终端可以暂时不部署或部分部署核心配置基线，或者允许某些核心配置项值暂时低于核心配置项基值进行部署。

10.7.3 整改计划

例外处理是一种临时性处理措施，应制定针对例外终端的有效整改计划，包括整改期限，整改措施，相关责任人等。整改计划经领导层审批后由管理层负责监督执行。

知识星球https://t.zsxq.com/JmiaeUR

附 录 A
（资料性附录）
身份鉴别配置要求示例

A.1 身份鉴别配置要求

依据 GB/T 22239—2008 中 7.1.3 对于第三级主机安全的要求，身份鉴别配置要求分为账户登录和口令管理两部分。

A.2 账户登录

账户登录具体配置要求如下：

a) 用户连续登录失败 5 次后锁定用户账户至少 60min。
b) 不显示上次登录到计算机的用户名。
c) 用户登录时应按 CTRL＋ALT＋DEL 进入安全登录界面。
d) 应设置用户登录安全警告提示。
e) 可使用智能卡登录本地，但智能卡移除时，应锁定计算机。
f) 应禁止无口令账户登录。
g) 限制批处理账户登录。

A.3 口令管理

口令管理具体配置要求如下：

a) 账户口令至少包含 8 个字符。
b) 口令最长有效期不能超过 90 d，最短有效期不低于 1 d。
c) 口令过期前 7 d 提示用户修改口令。
d) 更换口令时，新口令必须与先前历史记载的 8 个口令不匹配。
e) 口令复杂度必须符合下列最低要求：
   1) 不能包含用户账户名中超过两个连续字符的部分。
   2) 必须包含以下四类字符中的三类字符：
      ——英文大写字母(A～Z)；
      ——英文小写字母(a～z)；
      ——10 个基本数字(0～9)；
      ——非字母字符(例如!、$、#、%)。
f) 使用不可还原的 NT 加密方式来储存口令。

知识星球https://t.zsxq.com/JmiaeUR

附 录 B
（资料性附录）
核心配置清单

B.1 概述

本附录给出了 Windows 桌面操作系统关于身份鉴别配置要求核心配置部分清单。

B.2 配置清单

【产品名称】:Windows7 操作系统专业版

【配置项标识】:CGDCC-Win7-0001
【配置项名称】:账户锁定
【配置项描述】:此配置项指定锁定用户账户之前所允许的失败登陆尝试次数。在管理员重置锁定账户或账户锁定时间期满之前,无法使用该锁定账户。登录尝试失败次数设置范围介于 0～999 之间,0 代表永远不会锁定账户。
【配置项组别】:账户登录
【安全级别】:严重
【取值范围】:0～999 次
【配置项基值】:5 次
【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\AccountPolicies\AccountLockoutPolicy
【检查规则】:等于配置项基值

【配置编号】:CGDCC-Win7-0002
【配置项名称】:账户锁定时间
【配置项描述】:此安全设置指定到达“账户锁定阈值”后锁定账户在自动解锁之前保持锁定的分钟数。如果定义了账户锁定阈值,则账户锁定时间必须大于或等于重置时间。取值范围从 0～99 min,999 min,取值 0 代表账户将一直被锁定直到管理员明确解除对它的锁定。
【配置项组别】:账户登录
【安全级别】:严重
【取值范围】:0～99 999 min
【配置项基值】:15 min
【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\AccountPolicies\AccountLockoutPolicy
【检查规则】:等于配置项基值

【配置项标识】:CGDCC-Win7-0003
【配置项名称】:复位账户锁定计数器
【配置项描述】:此安全设置指定到达“账户锁定阈值”后锁定账户在自动解锁之前保持锁定的分钟

知识星球https://t.zsxq.com/JmiaeUR

数。如果定义了账户锁定阈值，则账户锁定时间必须大于或等于重置时间。取值范围从 0～99 min，999 min，取值 0 代表账户将一直被锁定直到管理员明确解除对它的锁定。

【配置项组别】：账户登录

【安全级别】：严重

【取值范围】：1～99 min，999 min

【配置项基值】：15 min

【赋值路径】：ComputerConfiguration\WindowsSettings\SecuritySettings\AccountPolicies\AccountLockoutPolicy

【检查规则】：等于配置项基值

【配置项标识】：CGDCC-Win7-0004

【配置项名称】：交互式登录：不显示最后的用户名

【配置项描述】：该安全设置确定是否在 Windows 登录屏幕中显示最后登录到计算机的用户的名称。如果启用该配置，则不会在“登录到 Windows”对话框中显示最后成功登录的用户的名称。如果禁用该配置，则会显示最后登录的用户的名称。

【配置项组别】：账户登录

【安全级别】：严重

【取值范围】：启用、禁用、未配置

【配置项基值】：启用

【赋值路径】：ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\SecurityOptions

【检查规则】：等于配置项基值

【配置项标识】：CGDCC-Win7-0005

【配置项名称】：交互式登录：无须按 Ctrl＋Alt＋Del

【配置项描述】：配置是否用户需要按 Ctrl＋Alt＋Del 才能登陆。禁用可以保用户输入口令时通过信任路径通信，可以防止截获用户口令攻击。

【配置项组别】：账户登录

【安全级别】：严重

【取值范围】：启用、禁用、未配置

【配置项基值】：禁用

【赋值路径】：ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\SecurityOptions

【检查规则】：等于配置项基值

【配置项标识】：CGDCC-Win7-0006

【配置项名称】：交互式登录：试图登录的用户的消息标题

【配置项描述】：该安全设置允许在包含“交互式登录：试图登录的用户的消息文本”的窗口的标题栏中显示标题的说明。

【配置项组别】：账户登录

【安全级别】：警告

【配置项基值】：警告

【赋值路径】：ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies

知识星球https://t.zsxq.com/JmiaeUR

\SecurityOptions

【检查规则】:等于

【配置项标识】:CGDCC-Win7-0007

【配置项名称】:交互式登录:试图登录的用户的消息文本

【配置项描述】:该安全设置指定用户登录时向其显示的文本消息。该文本通常用于法律原因,例如,警告用户滥用公司信息的后果或其操作可能要经过审核。

【配置项组别】:账户登录

【安全级别】:警告

【配置项基值】:“本系统仅供政务授权用户使用。未经授权或者越权使用的用户所有行为将被系统监督管理程序监控并记录。任何使用本系统的用户将会受到监控,一经发现有违法行为将其监控证据上交法律相关部门。”

【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\SecurityOptions

【检查规则】:等于配置项基值

【配置项标识】:CGDCC-Win7-0008

【配置项名称】:交互式登录:智能卡移除行为

【配置项描述】:配置当移除登录用户的智能卡时发生情况:①无操作②锁定工作站③强制注销④如果发生远程终端服务会话,则断开连接。

【配置项组别】:账户登录

【安全级别】:重要

【配置项基值】:锁定工作站

【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\SecurityOptions

【检查规则】:等于配置项基值

【配置项标识】:CGDCC-Win7-0009

【配置项名称】:账户:限制使用空白口令的本地账户只允许进行控制台登录

【配置项描述】:配置无口令保护的账户是否仅允许在本地登录。

【配置项组别】:账户登录

【安全级别】:重要

【配置项基值】:启用

【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\SecurityOptions

【检查规则】:等于配置项基值

【配置项标识】:CGDCC-Win7-0010

【配置项名称】:账户:限制使用空白口令的本地账户只允许进行控制台登录

【配置项描述】:配置无口令保护的账户是否仅允许在本地登录。

【配置项组别】:账户登录

【安全级别】:重要

【配置项基值】:启用

知识星球https://t.zsxq.com/JmiaeUR

【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\SecurityOptions
【检查规则】:等于配置项基值

【配置项标识】:CGDCC-Win7-0011
【配置项名称】:口令长度最小值
【配置项描述】:此配置确定账户口令包含的最少字符数。0 代表无口令设置。
【配置类型】:WMI 配置
【配置项组别】:口令管理
【安全级别】:严重
【取值范围】:0～24 位字符
【配置项基值】:8 位字符
【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\AccountPolicies\PasswordPolicy
【检查规则】:大于或等于配置项基值

【配置项标识】:CGDCC-Win7-0012
【配置项名称】:强制口令历史
【配置项描述】:配置最近历史口令存储个数,新设口令与存储历史口令不匹配时才能使用。防止口令重复出现频率过大造成不安定因素。取值范围在 0～24 之间,0 代表口令可以立即重复使用。
【配置项组别】:口令管理
【安全级别】:严重
【取值范围】:0～24 位字符
【配置项基值】:12 位字符
【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\AccountPolicies\PasswordPolicy
【检查规则】:大于或等于配置项基值

【配置项标识】:CGDCC-Win7-0013
【配置项名称】:口令复杂性要求
【配置项描述】:此配置用于对口令的复杂性进行规定要求。如启用该项配置则口令必须满足以下要求:1.不能包含用户名中超过两个连续字符部分。2.口令中需要包含以下字符中的四种:1)英文大写字母;2)英文小写字母;3)0～9;4)非字母字符(如!、#、%)。
【配置项组别】:口令管理
【安全级别】:严重
【取值范围】:启用、禁用和未配置
【配置项基值】:启用
【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\AccountPolicies\PasswordPolicy
【检查规则】:等于配置项基值

【配置项标识】:CGDCC-Win7-0014
【配置项名称】:口令最长使用期限

知识星球https://t.zsxq.com/JmiaeUR

【配置项描述】:该配置指定了口令过期之前的有效期天数,用来强制用户定期修改口令。该取值必须大于口令最短使用期限取值。取值范围在0～999 d之间,0代表永远不过期。

【配置项组别】:口令管理

【安全级别】:严重

【取值范围】:0～999 d

【配置项基值】:90 day

【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\AccountPolicies\PasswordPolicy

【检查规则】:小于或等于配置项基值

【配置项标识】:CGDCC-Win7-0015

【配置项名称】:口令最短使用期限

【配置项描述】:该配置指定用户口令保持有效的最短天数,可用来防止用户通过更改口令然后又将口令改回,从而绕过“口令最长使用期限”。其取值必须小于口令最长使用期限值,取值范围在1～998 d之间,0代表口令可以立即更改。

【配置项组别】:口令管理

【安全级别】:严重

【取值范围】:0～998 d

【配置项基值】:1 day

【赋值路径】:ComputerConfiguration\WindowsSettings\SecuritySettings\AccountPolicies\PasswordPolicy

【检查规则】:大于或等于配置项基值

【配置项标识】:CGDCC-Win7-0016

【配置项名称】:更改口令时不存储LAN管理器哈希值

【配置项描述】:此配置确定在更改口令时是否为新口令存储LAN管理器(LM)哈希值。LM哈希的加密性相对较弱的DES密钥和算法,易于受攻击。由于LM哈希存储在本地计算机上的安全数据库中,因此,一旦安全数据库受到攻击,口令便会泄漏。

【配置项组别】:口令管理

【安全级别】:严重

【取值范围】:启用、禁用和未配置

【配置项基值】:启用

【赋值路径】:HKLM\System\CurrentControlSet\Control\Lsa\NoLMHashComputerConfiguration\WindowsSettings\SecuritySettings\LocalPolicies\SecurityOptions

【检查规则】:等于配置项基值

知识星球https://t.zsxq.com/JmiaeUR

中 华 人 民 共 和 国
国 家 标 准
信息安全技术
政务计算机终端核心配置规范
GB/T 30278—2013
*
中 国 标 准 出 版 社 出 版 发 行
北京市朝阳区和平里西街甲 2 号(100029)
北京市西城区三里河北街 16 号(100045)
网址:www.gb168.cn
服务热线:400-168-0010
010-68522006
2014 年 5 月第一版
*
书号:155066·1-49171

版权专有 侵权必究

GB/T 30278-2013

知识星球https://t.zsxq.com/JmiaeUR