

The background features abstract, overlapping geometric shapes in shades of green and white. A large, light green shape with a white circular cutout is positioned in the upper right. A darker green shape is in the lower right. A vertical green bar is on the left side. The text is centered in the white space.

使用 UserLock 限制 Wi-Fi 和 VPN
会话 保障 Windows 网络的自带设
备安全

www.isdecisions.com

使用 UserLock 限制 Wi-Fi 和 VPN 会话 保障 Windows 网络的自带设备安全

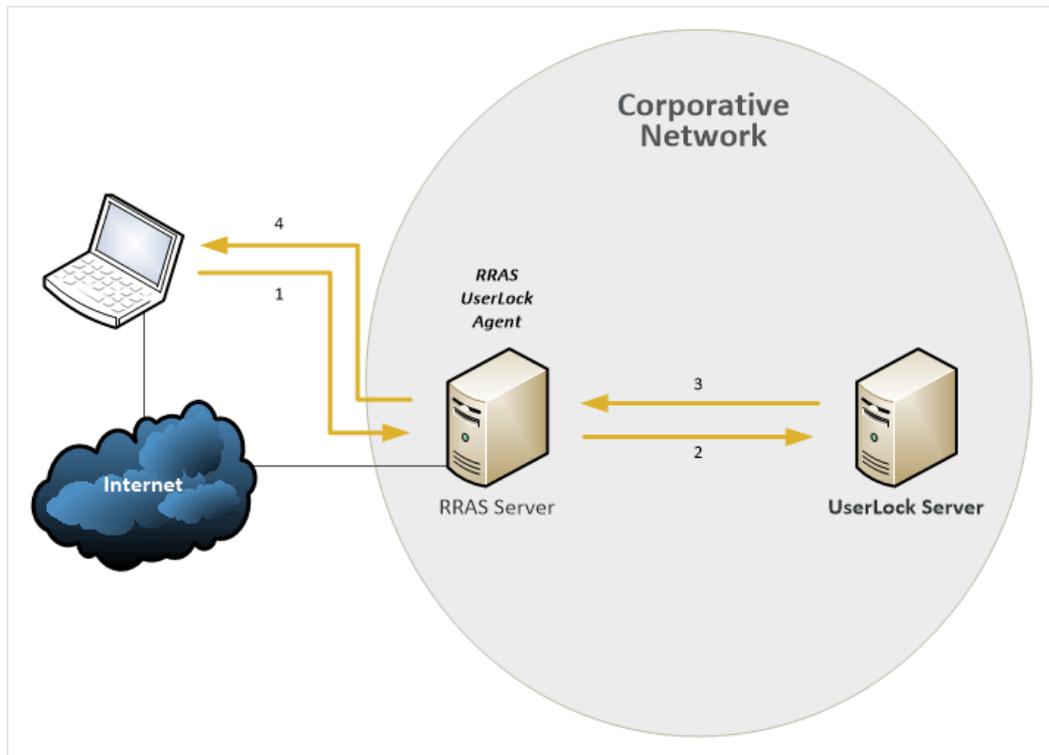
自带设备（即 **BYOD**，全称为 Bring Your Own Device）安全一直是很多 IT 部门关注的问题。知名网络安全监控软件 **UserLock** 最新版本（**UserLock7**）新增了对 **Wi-Fi 和 VPN 会话** 的监控功能，允许公司对他们的无线网络进行监控，确保有安全的 BYOD 环境。

使用 UserLock，公司可以对所有 Wi-Fi 和 VPN 会话进行**监控、限制和记录**。

如何使用 UserLock7 限制 Wi-Fi 和 VPN 会话

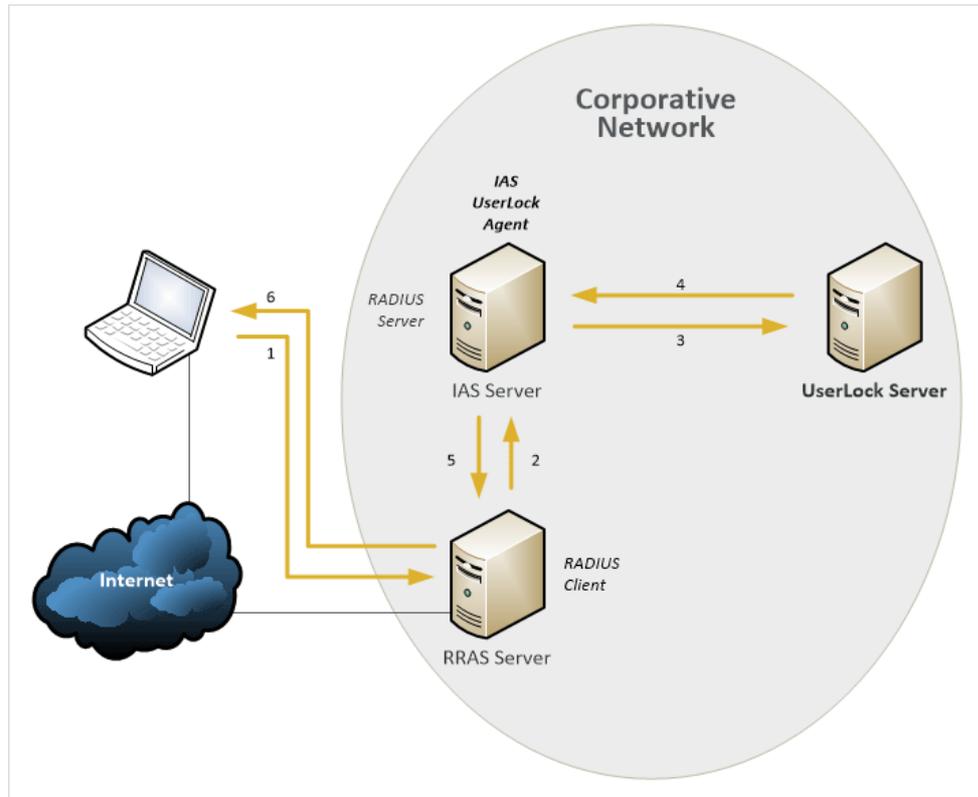
下面的简图显示了 UserLock 管理 RADIUS（RADIUS，即远程认证拨号用户服务，是一种认证协议。）认证的 VPN 和 Wi-Fi 会话的原理：

Windows 认证的 VPN

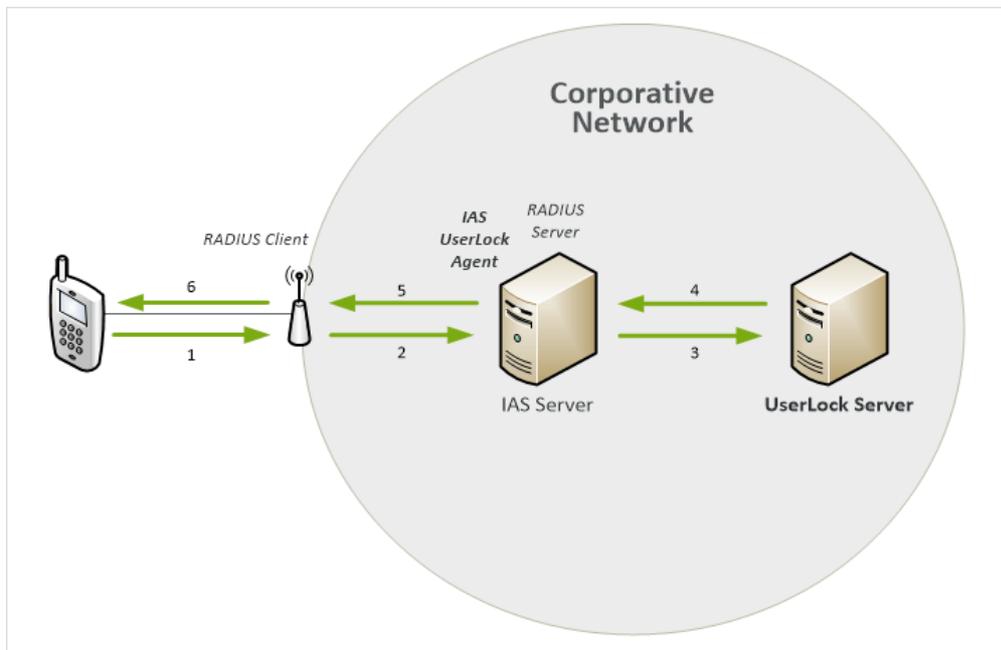


RADIUS 认证的 VPN



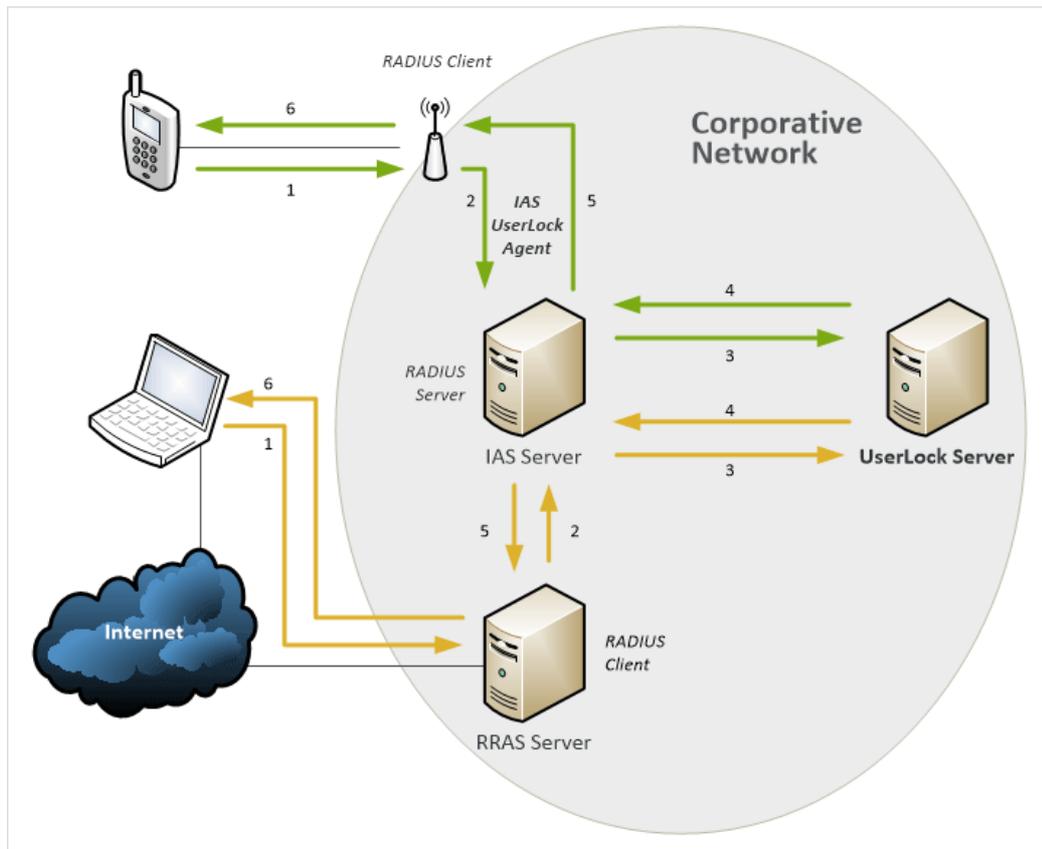


RADIUS 认证的 Wi-Fi



RADIUS 认证的 Wi-Fi 和 VPN





通过限制 Wi-Fi 和 VPN 会话，你能对网络访问进行更有效的监控。

为你的网络安装 UserLock 代理

要求：

- 对于 VPN 会话：经 RADIUS 服务器认证的 RRAS 服务器（RRAS，即路由与远程访问服务，是微软管理 VPN 会话的一种技术，RRAS 服务器可以与 Windows 认证或 RADIUS 认证进行配置。）或 VPN 服务器
- 对于 Wi-Fi 会话：访问点与 RADIUS 兼容

安装：

对于 VPN 会话：

- 在 RRAS 服务器上安装 RRAS UserLock 代理



- 或在认证 VPN 服务器的 RADIUS 服务器上安装 IAS (RADIUS) UserLock 代理

对于 Wi-Fi 会话:

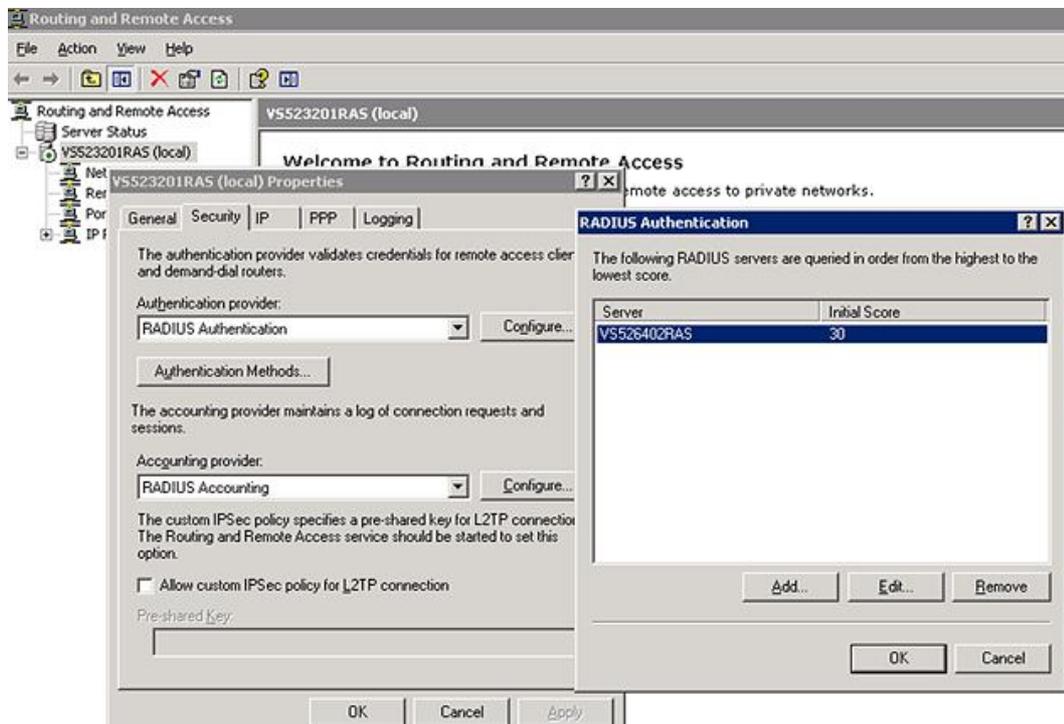
- 在认证 Wi-Fi 访问点的 RADIUS 服务器上安装 IAS (RADIUS) UserLock 代理

为受 UserLock 保护的帐户配置 Wi-Fi 和 VPN 限制。

使用:

在下面的案例中, 你可以看到如何为受保护的账户进行配置, 使对于所有用户都只允许一个 Wi-Fi 和 VPN 会话。

1. 为 VPN 服务器配置 RADIUS 认证指定的 IAS (RADIUS) 服务器 (名称和密码)。



2. 将 Wi-Fi 访问点设置为 RADIUS 认证指定的 IAS 服务器。



Wireless Settings

Wireless Band: IEEE802.11g

Mode: Access Point

Wireless Network Name(SSID): CORP

SSID Broadcast: Enable

Channel: 13 2.472 GHz Auto Channel Scan

Authentication: WPA-EAP

RADIUS Server Settings

Cipher Type: AUTO Group Key Update Interval: 1800

Primary radius server setting

RADIUS Server: 192.168.1.1

RADIUS Port: 1812

RADIUS Secret:

Secondary radius server setting

Secondary RADIUS Mode: Disable

RADIUS Server:

RADIUS Port: 1812

RADIUS Secret:

Primary accounting server setting

Accounting Mode: Enable

Accounting Server: 192.168.1.1

Accounting Port: 1813

3.在 IAS 服务器上安装 IAS UserLock 代理。

UserLock

← → · UserLock · Servers · SERVER1 · Agent distribution

Configuration

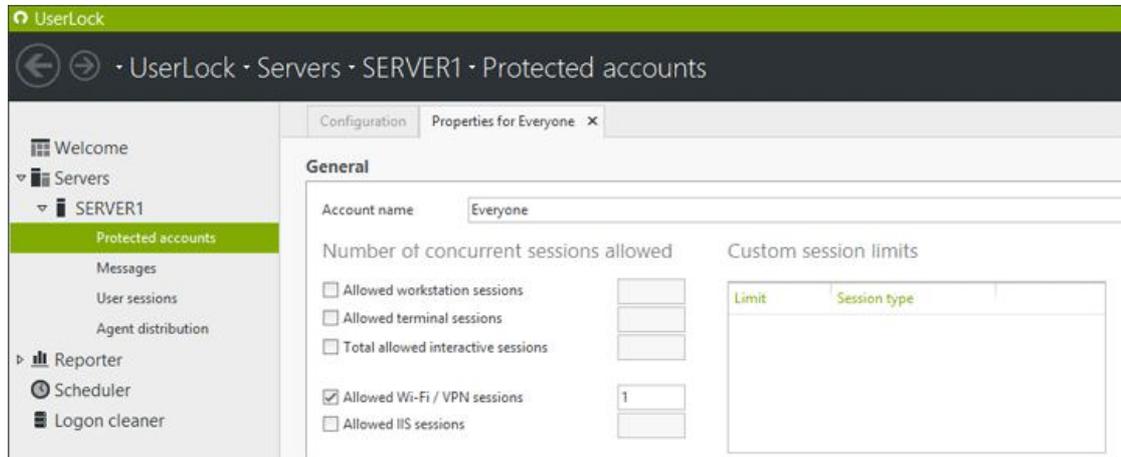
AGENT DISTRIBUTION SERVER1
All | 4 total | Automatic mode OFF

Computer	Agent status	Agent version	Roles
Agent type: Desktop			
Agent type: IAS			
SERVER1	Not installed		DC,RRAS,IA...
SERVER1	Not installed		DC,IAS,IIS 1
Agent type: IIS			
Agent type: RRAS			

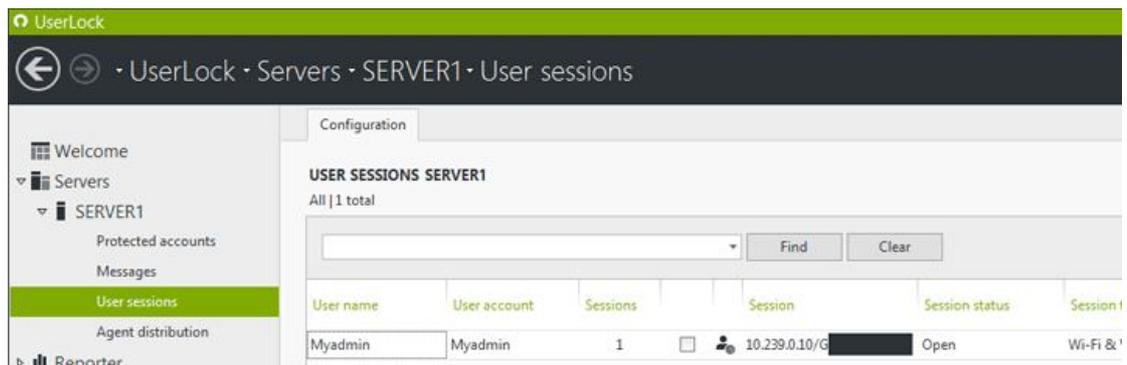
- Start Automatic mode
- Properties
- Refresh
- Display AD tree
- Enable auto filter
- Select all
- Unselect all
- All machines
- Only DC
- Only machines without agents
- Only unavailable machines
- Print data grid
- Install**
- Uninstall
- Reboot



4.将受保护的账号设为“Everyone”，使所有用户与新规则关联。勾选“允许 Wi-Fi 和 VPN 会话”并在后面的框中填写数字“1”。



5.将某个账户与 VPN 连接，连接成功后，你能在 UserLock 控制台看到会话。



6.试与该账户进行 Wi-Fi 连接，连接被拒绝。

7.关闭该账户与 VPN 的连接，再与 Wi-Fi 连接，连接被允许。

在 Wi-Fi 和 VPN 会话中，使用 UserLock 还可以对以下两方面进行限制：

- 定义工作时长
- 时间配额

